日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　３月３０日

出願番号
Application Number: 平成１１年特許願第０９０２５３号

出願人
Applicant (s): 沖電気工業株式会社

Japanese Patent Application
No. 11-090254
Filed 3/30/99
Attorney Docket: 32165-159044

１９９９年　８月２５日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３０５９６３６

【書類名】　特許願
【整理番号】　KK005703
【提出日】　平成11年 3月30日
【あて先】　特許庁長官　伊佐山　建志　殿
【国際特許分類】　H04N　1/387
【発明者】
　【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
　【氏名】　三井　靖博
【特許出願人】
　【識別番号】　000000295
　【氏名又は名称】　沖電気工業株式会社
　【代表者】　篠塚　勝正
【代理人】
　【識別番号】　100069615
　【弁理士】
　【氏名又は名称】　金倉　喬二
　【電話番号】　03-3580-7743
【手数料の表示】
　【予納台帳番号】　008855
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9001056
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像処理システム

【特許請求の範囲】

【請求項１】　正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイル及びその透かしキーを提供する画像提供装置と、

前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項２】　正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイルを提供する画像提供装置と、

正当な提供先からの画像ファイルであることを認証する機能の認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項３】　正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、これら画像ファイルと透かしキーを提供する画像提供装置と、

前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルと前記透かしキーを記憶しておき、適宜画像ファイルと透かしキーを利用

先に提供する画像管理装置と、

この画像管理装置から提供された透かしキーを用いて前記画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項４】　正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、

正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、この画像ファイルを利用先に提供する画像管理装置と、

正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項５】　正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、

正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶し

ておき、正当な提供先からの画像ファイルであることを認証する認証情報を含む付随情報を画像ファイルに付随させ、利用先から画像ファイルのアクセスがあった場合に、その画像ファイルとともに付随情報を利用先に提供する画像管理装置と、

付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを特徴とする画像処理システム。

【請求項６】　請求項１において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを特徴とする画像処理システム。

【請求項７】　請求項３において、画像管理装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを特徴とする画像処理システム。

【請求項８】　請求項３において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを特徴とする画像処理システム。

【請求項９】　請求項３において、画像管理装置は、提供された透かしキーに含まれる認証情報を画像ファイルに付随する付随情報に含めて、その付随情報を画像ファイルとともに利用先に提供し、画像利用装置では、付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出して改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用するようにしたことを特徴とする画像処理システム。

【請求項１０】　請求項１から請求項９のいずれかにおいて、認証情報には、画像ファイルの提供先を識別する提供先識別情報又は画像ファイルを識別する画像識別情報を含むことを特徴とする画像処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像処理システムに関し、さらに詳しくは、画像の改竄防止を実現する画像処理システムに関する。なお、改竄とは、改変又は置換の２つを意味する。改変とは、画像の中身を構成するデータの値を変更することをいう。置換とは、画像を別のデータと置き換えることをいう。

【０００２】

【従来の技術】

従来の画像処理システムでは、画像の管理は、基本的に画像保管・処理装置におけるアクセスコントロールによって行われていた。アクセス許可を管理する方法では、画像ファイルの書き込みを禁止し読み出しのみを可能にする等の制限を行って改竄を不能にすることによって行われていた。また、暗号化による管理方法では、暗号システムと組み合わせたシステムを構成し、画像を暗号化して復号キーと暗号化画像を保管し、復号キーがなければ暗号化画像が復号できず、復号できなければ処理ができないという方法によって行われていた。

【０００３】

また、画像自体の暗号化とは別に、画像の改竄を検出する方法として、画像データからメッセージ・ダイジェスト、圧縮子やハッシュ値と呼ばれるデータの指紋とも呼ぶべき特徴的なビット・パターンを検証データとして作成して画像とは別に管理し、検証時に検証しようとする画像から検証データを作成し、その値と管理してあった検証データを比較し、異なる場合は改竄が行われているという検証方法もあった。このような検証データを作成するメッセージ・ダイジェスト関数としてもっとも広く使用されているのは、ＲＳＡ社（米）のＭＤ２，ＭＤ４，ＭＤ５といった一連のアルゴリズムである。

【０００４】

検証データを作成して、検証時にその値の比較によって改竄を検出するシステムでも、改竄画像から検証データを作成し、画像と検証データの両方を摩り替えることによって欺く事ができるため、検証データは必ず暗号化されて使用される。

暗号システムでは、一般的に、暗号化と復号化を共通の秘密鍵（secret key）で行う「共通鍵システム」、公開されている公開鍵（public key）とその鍵の所有者以外には秘密にされている秘密鍵（private key ）が使用され、一方の鍵で暗号化し他方の鍵で復号化する「公開鍵システム」が使用され、それに加えて認証を行うための電子署名が使用される。「共通鍵システム」として代表的なものにＤＥＳ（Data Encryption Standard）システム、日本電信電話株式会社のＦＥＡＬ（Fast Encryption Algorithm ）システム、三菱電機株式会社のＭＩＳＴＹシステム等があり、「公開鍵システム」として代表的なものにＲＳＡ社（米）のＲＳＡ公開鍵システムがある。

【０００５】

また、電子透かし技術はこれまで、日経エレクトロニクス 1997.2.24(no.683)に述べられているように、これまでの適用範囲のほとんどは「著作権保護」の為であり、画像品質を損なわないように、そして埋め込んだ透かしができるだけ消えないような実現方法が数多く提案されてきた。この利用方法は、知覚し難く、画像に変更を加えても消え難い電子透かしを使って、情報を埋め込み、その情報を確認することによって著作権を確認するというものであった。

【０００６】

電子透かしの画像検証に対する適用として、特開平10-208026 号公報に述べられるように、電子透かしの一つの特徴であるステガノグラフィー（データ隠蔽）によって、スタンピング情報を元画像に埋め込み、その情報を抽出し、比較することによって、改竄を検出するという技術も提案されている。

電子透かしによる情報埋め込みはさまざまな用途が提案されており、著作権情報以外にも、画像を作成した装置情報や、作成者情報、使用者情報等のさまざまな管理情報を画像内に電子透かしに埋め込むシステムが提案されている。

【０００７】

【発明が解決しようとする課題】

しかしながら、アクセス権だけの操作では、特権ユーザーによる改竄は防止できず、また、画像を扱うすべての装置の完全なアクセス権設定を実現することはコストのかかる作業が必要であった。

暗号化による画像管理では、画像ファイル自体を暗号化しているために、画像を表示するたびに、復号化（及び再暗号化）の処理を行う必要があった。このため、特に、多量の画像を処理するシステムではその処理負荷が大きくなってしまう問題点があった。また、画像がシステム内に分散した複数のマシンで利用されるシステムでは、各マシン毎に復号化（及び再暗号化）の処理が行われる為に、その処理の過程及び暗号・復号鍵の管理並びに復号された画像の管理が万全であることは記しがたく、セキュリティの甘いマシンを選んで不正を行いやすいという問題点があった。

【０００８】

さらに、メッセージ・ダイジェストといった検証データを用いて改竄を検出する場合でも、検証データの管理に関して、検証データの保証を行うために、検証データを管理する暗号システムが必要であり、上記の画像の暗号化と同様の問題が生じていた。

【０００９】

【課題を解決するための手段】

本発明の請求項１に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイル及びその透かしキーを提供する画像提供装置と、前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【００１０】

請求項２に記載の発明は、正当な提供先からの画像ファイルであることを認証

する認証情報を含む透かしキーを用いて電子透かし情報が抽出可能な画像ファイルを提供する画像提供装置と、正当な提供先からの画像ファイルであることを認証する機能の認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【００１１】

請求項３に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、これら画像ファイルと透かしキーを提供する画像提供装置と、前記画像提供装置から提供された透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルと前記透かしキーを記憶しておき、適宜画像ファイルと透かしキーを利用先に提供する画像管理装置と、この画像管理装置から提供された透かしキーを用いて前記画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【００１２】

請求項４に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された

画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、この画像ファイルを利用先に提供する画像管理装置と、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【００１３】

請求項５に記載の発明は、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて抽出可能な電子透かし情報を画像ファイルに埋め込み、この画像ファイルを提供する画像提供装置と、正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを生成し、この透かしキーを用いて前記画像提供装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを記憶しておき、正当な提供先からの画像ファイルであることを認証する認証情報を含む付随情報を画像ファイルに付随させ、利用先から画像ファイルのアクセスがあった場合に、その画像ファイルとともに付随情報を利用先に提供する画像管理装置と、付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出し、透かしキーの認証情報を用いて透かしキーの改竄の有無を判断するとともに、改竄の有無を判断した透かしキーを用いて画像ファイルの改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用する画像利用装置とを備えたことを構成上の特徴とする画像処理システムを提供する。

【００１４】

請求項６に記載の発明は、請求項１において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを構成上の特徴とする画像処理システムを提供する。

請求項７に記載の発明は、請求項３において、画像管理装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを構成上の特徴とする画像処理システムを提供する。

【００１５】

請求項８に記載の発明は、請求項３において、画像利用装置では、正当な提供先からの画像ファイルであることを認証する認証情報を生成し、この認証情報と、提供された透かしキーから抽出した認証情報とを比較して提供された透かしキーの正当性を認証することを構成上の特徴とする画像処理システムを提供する。

請求項９に記載の発明は、請求項３において、画像管理装置は、提供された透かしキーに含まれる認証情報を画像ファイルに付随する付随情報に含めて、その付随情報を画像ファイルとともに利用先に提供し、画像利用装置では、付随情報から認証情報を認識して、この認証情報を含む透かしキーを生成し、この透かしキーを用いて画像管理装置から提供された画像ファイルから電子透かし情報を抽出して改竄の有無を判断し、改竄の有無を判断した画像ファイルを利用するようにしたことを構成上の特徴とする画像処理システムを提供する。

【００１６】

請求項１０に記載の発明は、請求項１から請求項９のいずれかにおいて、認証情報には、画像ファイルの提供先を識別する提供先識別情報又は画像ファイルを識別する画像識別情報を含むことを構成上の特徴とする画像処理システムを提供する。

なお、認証情報の提供先識別情報には、例えば、提供先の画像提供装置を識別する装置識別情報、提供先の画像提供装置のＭＡＣアドレス、提供先の画像提供装置が所属するシステムを識別するシステム識別情報や画像ファイルの作成者を識別する作成者識別情報がある。提供先識別情報は、データサイズ可変なハッシ

ュ値で表すようにしてもよい。また、認識情報の画像識別情報には、例えば、画像提供装置が画像ファイルを画像利用装置に提供する毎に繰り上がるカウント数、画像提供装置が画像ファイルを画像利用装置に提供する毎に一方向ハッシュ関数によって更新するハッシュ値、画像提供装置が画像ファイルファイルを作成したファイル作成時間等の時間情報がある。また、請求項６又は請求項９に記載の付随情報には、例えば、画像ファイルのファイル名がある。

【００１７】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態を説明する。なお、これによりこの発明が限定されるものではない。

第１の実施の形態

図１は、第１の実施の形態の画像処理システムのネットワーク構成図である。

【００１８】

この画像処理システムでは、画像入力装置１０１(1) ～(M) で取り込まれた画像は、画像処理装置１０２(1) ～(M) 、画像管理サーバ１０３及びネットワーク１０４を介して画像表示装置１０５(1) ～(N) のそれぞれで表示されるようになっている。なお、以下の説明では、画像入力装置１０１(1) ～(M) のｍ番目を画像入力装置１０１(m) とし、画像処理装置１０２(1) ～(M) のｍ番目を画像処理装置１０２(m) とし、画像表示装置１０５(1) ～(N) のｎ番目を画像表示装置１０５(n) とする。

【００１９】

前記画像入力装置１０１(m) は、画像を取り込んで電子データ化する装置であり、通常スキャナや電子カメラによって構成され、取り込まれた画像データを元画像Ａ(m) として出力する。

前記画像処理装置１０２(m) は、前記画像入力装置１０１(m) からの元画像Ａ(m) をそれぞれ入力し、この元画像Ａ(m) に電子透かしを埋め込んだ原本画像Ｃ(m) と暗号化した透かしキーｂ22(m) を対にして出力する機能を有する。

【００２０】

図２に、第１の実施の形態の画像処理装置の機能ブロック構成図を示す。この

画像処理装置１０２(m) は、電子透かし埋め込み部２１(m) と透かしキー生成部２２(m) と暗号部２３(m) とを有している。前記電子透かし埋め込み部２１(m) は、元画像Ａ(m) に対する改竄を検出するための電子透かしを透かしキーＢ22(m) を用いて元画像Ａ(m) に埋め込んだ原本画像Ｃ(m) を出力する。前記透かしキー生成部２２(m) は、前記透かしキーＢ22(m) を生成する。ここで、透かしキーＢ22(m) は、本実施の形態では、電子透かしの埋め込み・検証の両方に使用できる共通キーとして説明するが、埋め込みと検証とが相違するようにしてもよい。

【００２１】

なお、元画像Ａ(m) と原本画像Ｃ(m) と透かしキーＢ22(m) が簡単に手に入るとすると、いろいろな元画像Ａ(m) とその原本画像Ｃ(m) の差分と透かしキーＢ22(m) の関係を調べることによって、電子透かしの埋め込み方式の解析が容易になり、原本画像Ｃ(m) の改竄や偽造の容易性を高めることになる。このため、透かしキーＢ22(m) はオリジナルの状態で流通しないシステム構成が好ましく、ここでは、透かしキーＢ22(m) の生成にＲＳＡ等の公開鍵システムを用いて、透かしキーＢ22(m) のやり取りを行う場合を想定する。

【００２２】

図３に、第１の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部２２(m) は、認証情報生成手段２４(m) と透かしキー生成手段２５(m) とを有している。前記認証情報生成手段２４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置１０２(m) を識別するための装置識別値Ｄ24a(m)と元画像Ａ(m) を識別するための画像識別値Ｄ24b(m)とを使用する。また、認証情報生成手段２４(m) には、装置識別値Ｄ24a(m)を記憶する装置識別値記憶部２４ａ(m) と、元画像Ａ(m) をナンバリングするための画像識別値Ｄ24b(m)を元画像Ａ(m) の処理毎に繰り上がるカウント数として出力する画像カウンタ２４ｂ(m) とを備えてある。前記透かしキー生成手段２５(m) は、装置識別値Ｄ24a(m)と画像識別値Ｄ24b(m)とを含む透かしキーＢ22(m) を生成する。例えば、装置識別値Ｄ24a(m)を「ＫＫ

Ｋ　ＦＪＩ１２３」とし、画像識別値Ｄ24b(m)を「０１２３４５６７」とした場合、単純にそれぞれを繋ぎ合わせた「ＫＫＫ　ＦＪＩ１２３０１２３４５６７」を含む透かしキーＢ22(m) を生成する。なお、装置識別値Ｄ24a(m)としては、画像処理装置１０２(m) 内のソフトウェアやハードウェアに設定した値を使用することができる。

【００２３】

図２に戻って、前記暗号部２３(m) は、透かしキーＢ22(m) を暗号化して透かしキーｂ22(m) を出力する。そして、画像処理装置１０２(m) は、原本画像Ｃ(m) と透かしキーｂ22(m) とを対にして出力する。

図１に戻って、前記画像管理サーバ１０３は、前記画像処理装置１０２(m) から送られてきた原本画像Ｃ(m) と透かしキーｂ22(m) を保存・管理するサーバであり、通常のデータベースやワークフローシステムとして構築され、原本画像Ｃ(m) と透かしキーｂ22(m) とを対にして管理する。

【００２４】

図４に、第１の実施の形態の画像管理サーバの機能ブロック構成図を示す。この画像管理サーバ１０３は、電子透かし検証部３１と、認証情報・検出検証部３３と、認証情報生成手段３４(1) ～(M) （以下、m番目を認証情報生成手段３４(m) という。）と、復号部３６と、記憶制御部３７と、暗号部３８とを有している。前記電子透かし検証部３１は、画像処理装置１０２(m) から提供された原本画像Ｃ(m) を提供された透かしキーＢ22(m) を用いて電子透かしが抽出できるか否かを検証する。透かしキーＢ22(m) が正当なものである場合、原本画像Ｃ(m) から電子透かしが抽出できても改竄が検出されれば改竄が行われているということが分かり、抽出できなければ原本画像Ｃ(m) が置換されていることが分かる。前記認証情報・検出検証部３３は、透かしキーＢ22(m) から前記装置識別値Ｄ24a(m)及び前記画像識別値Ｄ24b(m)を抽出し、各認証情報生成手段３４(m) で生成される装置識別値Ｄ34a(1)～(M) （以下、m番目を装置識別値Ｄ34a(m)という。）と画像識別値Ｄ34b(1)～(M) （以下、m番目を画像識別値Ｄ34b(m)という。）と比較を行うことによって、提供された透かしキーＢ22(m) が正当なものであるかどうかを検証する。前記認証情報生成手段３４(m) は、正当な提供先からの画

像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置１０２(m) を識別するための前記装置識別値Ｄ24a(m)と同一の装置識別値Ｄ34a(m)と、元画像Ａ(m) を識別するための前記画像識別値Ｄ24b(m)と同一の画像識別値Ｄ34b(m)とを使用する。また、前記認証情報生成手段３４ (m) には、装置識別値Ｄ34a(m)を記憶する装置識別値記憶部３４ａ(m) と、元画像Ａ(m) をナンバリングするための画像識別値Ｄ34b(m)を原本画像Ｃ(m) の処理毎に繰り上がるカウント数として出力する画像カウンタ３４ｂ(m) とを備えてある。なお、装置識別値Ｄ34a(m)の装置識別値記憶部３４ａ(m) への記憶や画像カウンタ３４ｂ(m) のセットは、システム運用開始時又は運用中に予め行っておく。

【００２５】

前記復号部３６は、画像処理装置１０２(m) から送られてきた暗号化された透かしキーｂ22(m) を元の透かしキーＢ22(m) に復号する。前記記憶制御部３７は、原本画像Ｃ(m) と透かしキーＢ22(m) とを対にして管理する。前記暗号部３８は、前記画像表示装置１０５(n) 毎に応じて透かしキーＢ22(m) を暗号化した透かしキーｂ22(n) を生成する。そして、画像管理サーバ１０３は、原本画像Ｃ(m) とともに透かしキーｂ22(n) をそれぞれ対にして、各画像表示装置１０５(n) に送る（図１参照）。なお、ここでは、画像処理装置１０２(m) で処理された原本画像Ｃ(M) が、画像管理サーバ１０３を介して画像表示装置１０５(n) まで送られ表示される場合は、画像処理装置１０２(m) での画像処理回数と画像表示装置１０５(n) での表示回数が同じであることを想定する。この想定は、以下の各実施の形態でも同様とする。

【００２６】

図１に戻って、前記ネットワーク１０４は、例えば、ＬＡＮやＷＡＮ等で構築されるネットワークである。前記画像表示装置１０５(n) は、原本画像Ｃ(m) を表示利用する装置である。

図５に、第１の実施の形態の画像表示装置の機能ブロック構成図を示す。この画像表示装置１０５(n) は、電子透かし検証部５１(n) と、認証情報抽出・検証

部５３(n) と、認証情報生成手段５４(1) ～(M) （以下、m番目を認証情報生成手段５４(m) という。）と、復号部５６(n) と、表示制御部５９(n) とを有している。前記電子透かし検証部５１(n) は、画像管理サーバ１０３から提供された原本画像Ｃ(m) を提供された透かしキーＢ22(m) を用いて電子透かしが抽出できるか否かを検証する。透かしキーＢ22(m) が正当なものである場合、原本画像Ｃ(m) から電子透かしが抽出できても改竄が検出されれば改竄が行われているということが分かり、抽出できなければ原本画像Ｃ(m) が置換されていることが分かる。前記認証情報・検出検証部５３(n) は、透かしキーＢ22(m) から前記装置識別値Ｄ24a(m)及び前記画像識別値Ｄ24b(m)を抽出し、認証情報生成手段５４(n) で生成される装置識別値Ｄ54a(m)と画像識別値Ｄ54b(m)と比較を行うことによって、提供された透かしキーＢ22(m) が正当なものであるかどうかを検証する。前記認証情報生成手段５４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置１０２(m) を識別するための前記装置識別値Ｄ24a(m)と同一の装置識別値Ｄ54a(m)と元画像Ａ(m) を識別するための前記画像識別値Ｄ24b(m)と同一の画像識別値Ｄ54b(m)とを使用する。また、前記認証情報生成手段５４(m) には、装置識別値Ｄ54a(m)を記憶する装置識別値記憶部５４ａ(m) と、元画像Ａ(m) が送られて来た順番をナンバリングするための画像識別値Ｄ54b(m)を原本画像Ｃ(m) の処理毎に繰り上がるカウント数として出力する画像カウンタ５４ｂ(m) とを備えてある。なお、装置識別値Ｄ54a(m)の装置識別値記憶部５４ａ(m) への記憶や画像カウンタ５４ｂ(m) のセットは、システム運用開始時又は運用中に予め行っておく。

【００２７】

前記復号部５６(n) は、画像管理サーバ１０３から送られてきた暗号化された透かしキーｂ22(n) を元の透かしキーＢ22(m) に復号する。前記表示制御部５９(n) は、提供された原本画像Ｃ(m) を図示しないＣＲＴ等の表示部に表示させる。

次に、上記構成の画像処理システムの画像処理の流れを説明する。図１～図５

を適宜参照するものとする。

【００２８】

まず、画像入力装置１０１(m) によって取り込まれた電子データ化した元画像Ａ(m) は、画像処理装置１０２(m) に入力される。

次に、画像処理装置１０２(m) では、透かしキー生成部２２(m) で電子透かしの埋め込みのための透かしキーＢ22(m) を生成し、その透かしキーＢ22(m) を使用して電子透かし埋め込み部２１(m) で電子透かしを埋め込んだ原本画像Ｃ(m) を生成する。また、画像処理装置１０２(m) では、暗号部２３(m) が、画像管理サーバ１０３の公開鍵を使用して生成した透かしキーＢ22(m) を透かしキーｂ22(m) に暗号化する。そして、画像処理装置１０２(m) は、原本画像Ｃ(m) と透かしキーｂ22(m) とを対にして画像管理サーバ１０３に送る。

【００２９】

次に、画像管理サーバ１０３では、復号部３６が送られてきた透かしキーｂ22(m) を画像管理サーバ１０３の秘密鍵を用いて復号し、電子透かし検証部３１が復号された透かしキーＢ22(m) を使用して原本画像Ｃ(m) の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像Ｃ(m) の改竄が行われていないということの確認を行う。また、画像管理サーバ１０３では、認証情報・検出検証部３３が、復号された透かしキーＢ22(m) から装置識別値Ｄ24a(m)及び画像識別値Ｄ24b(m)を分離し、認証情報生成手段３４(m) によって生成される装置識別値Ｄ34a(m)及び画像識別値Ｄ34b(m)のそれぞれと比較する。この比較の結果、装置識別値Ｄ24a(m)と装置識別値Ｄ34a(m)とが一致するとともに画像識別値Ｄ24b(m)と画像識別値Ｄ34b(m)とが一致した場合には、提供された透かしキーＢ22(m) が正当な提供者から提供された正当なものであると判断する。なお、両方とも一致しない場合や一方が一致しない場合は、正当な提供先からの透かしキーＢ22(m) が改竄された不正なものであると判断する。さらに、画像管理サーバ１０３では、前記記憶制御部３７が改竄の行われていない原本画像Ｃ(m) と透かしキーＢ22(m) とを対にして管理する。ここで、画像管理サーバ１０３は、電子透かしが抽出できない場合や電子透かしが抽出できたが改竄が検出された場合には、その原本画像Ｃ(m) は正当なものでないため、改竄検出の警告を表示等により報知

して、その原本画像Ｃ(m) の表示を行わないことで、改竄画像による不正を防止できる。そして、前記画像表示装置１０５(n) から原本画像Ｃ(m) の転送を要求されたり自動的に転送する場合には、画像管理サーバ１０３は　前記暗号部３８で、前記画像表示装置１０５(n) 毎に応じて透かしキーＢ22(m) を暗号化した透かしキーｂ22(n) を生成し、原本画像Ｃ(m) とともにその透かしキーｂ22(n) をそれぞれ対にして各画像表示装置１０５(n) に送る。

【００３０】

各画像表示装置１０５(n) では、復号部５６(n) が送られてきた透かしキーｂ22(n) を画像表示装置１０５(n) の秘密鍵を用いて復号し、電子透かし検証部51(n) が復号された透かしキーＢ22(m) を使用して原本画像Ｃ(m) の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像Ｃ(m) の改竄が行われていないということの確認を行う。また、画像表示装置１０５(n) では、認証情報・検出検証部５３(m) が、復号された透かしキーＢ22(m) から装置識別値Ｄ24a(m)及び画像識別値Ｄ24b(m)を分離し、認証情報生成手段５４(m) によって生成される装置識別値Ｄ54a(m)及び画像識別値Ｄ54b(m)のそれぞれと比較する。この比較の結果、装置識別値Ｄ24a(m)と装置識別値Ｄ54a(m)とが一致するとともに画像識別値Ｄ24b(m)と画像識別値Ｄ54b(m)とが一致した場合には、提供された透かしキーＢ22(m) が正当な提供者から提供された正当なものであると判断する。なお、両方とも一致しない場合や一方が一致しない場合は、正当な提供先からの透かしキーＢ22(m) が改竄された不正なものであると判断する。さらに、画像管理サーバ１０３では、提供された原本画像Ｃ(m) が改竄されていないことが判明すれば、前記表示制御部５９(n) は、原本画像Ｃ(m) を図示しないＣＲＴ等の表示部に表示させる。

【００３１】

したがって、画像表示装置１０５(n) は、電子透かしが抽出できない場合や電子透かしが抽出できたが改竄が検出された場合には、その原本画像Ｃ(m) は正当なものでないため、改竄検出の警告を表示等により報知して、その原本画像Ｃ(m) の表示を行わないことで、改竄画像による不正を防止できる。

上記第１の実施の形態によれば、画像を利用する際に画像表示しか行わない画

像処理装置において、改変検出可能な電子透かしを埋め込んだ原本画像と、認証情報を含む透かしキーとを提供し、提供先で透かしキーを使用して原本画像から電子透かしを抽出するようにしたため、原本画像の改竄を検出することが可能になる。また、提供先において、認証情報を含む透かしキーから認証情報を取り出し、また、透かしキーが正当であれば取り出した認証情報と同一の認証情報を生成して、互いに比較することで透かしキーの正当性を認証することができる。このため、提供された透かしキーを用いて提供された原本画像から電子透かしが抽出できない場合に、透かしキーの正当性が確認されていなければ、原本画像自体に改竄が行われたのか又は透かしキーに改竄が行われたのかを判別することができないが、本実施の形態のように透かしキーの正当性が確認されれば、原本画像に何らかの改竄があることを判別することができるようになる。したがって、本実施の形態では、他の認証機構を導入する必要がなく、画像処理装置の成りすましや、画像の摩り替えに対するセキュリティを向上することができる。

【００３２】

また、本実施の形態では、従来のように画像を暗号化して管理し、復号しなければ表示できない暗号システムに比べると、画像を画像データとして管理できるため画像データ管理部分は通常の画像処理システムと同等に構成でき、一度原本画像を作成した後は、特に、オリジナルの元画像データは作成されることがない場合には、画像の改変を高度に防ぐことが可能となる。

【００３３】

なお、上記第１の実施の形態では、透かしキーを暗号化して転送を行う例を示したが、透かしキーは、電子透かしを埋め込む際にも使用するが、電子透かしを埋め込んだ原本画像作成後は、電子透かしを抽出し検証するためにだけ使用するキーであり、暗号システムにおける復号鍵とは異なり、元画像に戻す為の鍵ではないため、その管理を復号鍵に比べて緩いものにできるという特徴もある。画像入力装置と画像処理装置と画像管理サーバが、いわゆる対タンパ性を持つ一体された高いセキュリティな装置である場合、例えば、外部からハッキングされない、内部を見ることができない又はシステム等を破壊されない装置である場合、元画像データが搾取される可能性が低いため、透かしキーの機密性を緩めることが

可能であり、オリジナルのままで移動させても問題は少ない。ただし、透かしキーによる原本画像の検証が成立したとしても、原本画像と透かしキーの両方を偽造したものと摩り替えることによって電子透かしの検証を成立させることもできる。原本画像又は透かしキーだけが不当なものに摩り替えられたとしても、検証が成立せずに露見する。原本画像が正当なもので、画像の摩り替えも改変も行われていない、つまり改竄されていないことを示す為には、まず、透かしキーが正当なものであり、その透かしキーを用いて原本画像から電子透かしが抽出され、その後、電子透かしの検証によって画像の改竄が検出されないことが必要である。

【００３４】

電子透かしの検証を成立させる偽造した原本画像と透かしキーの作成の可能な方法の一つとして画像処理装置を不正利用し、その画像処理装置を用いて作成した原本画像・透かしキーと摩り替える方法がある。処理がソフトウェアで行われるのであれば、そのソフトウェアを盗み出し不正利用することが可能である。しかし、本実施の形態では、この画像処理装置がセキュリティの要であり、これが盗まれなければ問題の起きる可能性は非常に低くなる。また、透かしキー生成部と電子透かし埋め込み部をハードウェアにインプリメントし、処理を隠蔽し、盗まれにくくすることであるが、コスト及び実現の容易性を考えると、ソフトウェアにおけるインプリメントの処理における対策も必要である。このため、本実施の形態のように、認証情報を含む透かしキーを使用することで、原本画像及び透かしキーを送ってきた画像処理装置が正当なものであるという認証を行うことができるようになる。

【００３５】

第２の実施の形態

以下、上記第１の実施の形態との相違点を説明する。本第２の実施の形態は、上記第１の実施の形態と比較して透かしキーに含まれる認証情報の内の画像識別値を画像カウンタのカウント数ではなく、画像ファイル毎にラベリングするハッシュ値とした。なお、ハッシュ値とするのは、どのような認証情報に対しても行うことが可能であり、それらの説明は省略する。また、画像処理システムのネッ

トワークは、上記第１の実施の形態の場合を想定し、その説明は省略する。

【００３６】

図６に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部２２(m) は、認証情報生成手段２４(m) と透かしキー生成手段２５(m) とを有している。前記認証情報生成手段２４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置を識別するための装置識別値Ｄ24a(m)と、元画像Ａ(m) を識別するための画像識別値Ｄ24c(m)とを使用する。この画像識別値Ｄ24c(m)が、本第２の実施の形態では、ハッシュ値としたのである。このハッシュ値は、一方向ハッシュ関数により生成される。一方向ハッシュ関数としては、例えば、ＲＳＡ社（米）のＭＤ４，ＭＤ５やＳＨＡ（Secure Hash Algorithm ）等がある。

【００３７】

このため、前記認証情報生成手段２４(m) には、装置識別値Ｄ24a(m)を記憶する装置識別値記憶部２４ａ(m) と、元画像Ａ(m) をナンバリングするための画像識別値Ｄ24c(m)を元画像Ａ(m) の処理毎にハッシュ値を生成するハッシュ値生成部２４ｃ(m) とを備えてある。前記透かしキー生成手段２５(m) は、装置識別値Ｄ24a(m)及びハッシュ値としての画像識別値Ｄ24c(m)を含む透かしキーＢ22(m) を生成する。なお、ハッシュ値を生成するには、初期値ｃ(m) が必要であり、この初期値ｃ(m) は、システム運用開始時等に予め設定しておく。そして、運用が開始されると、ハッシュ値生成部２４ｃ(m) は初期値ｃ(m) からハッシュ値を生成し、その後はフィードバックされる一つ前の画像に対して生成されたハッシュ値から現画像のハッシュ値を作成し、透かしキー生成手段２５(m) はその値から透かしキーＢ22(m) を生成することになる。

【００３８】

なお、上述した前記透かしキー生成部２２(m) の認識情報生成手段２４(m) は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省

略する。また、画像管理サーバや画像入力装置にも、一方向ハッシュ関数の初期値は、システム運用開始時に予め設定しておけばよいが、初期値として画像処理装置の装置識別値を使用してもよい。この場合、画像管理サーバや画像表示装置では、装置識別値を入力するだけで初期値も設定することができる。また、画像管理サーバと画像表示装置との間のやり取りで透かしキーを替えるような場合には、画像処理装置と画像管理サーバとの間で使用するハッシュ値の設定は画像管理サーバのみ装置識別値の入力を行えばよいことになる。

【００３９】

本第２の実施の形態では、ハッシュ値により生成した認証情報を含む透かしキーとしたため、一方向ハッシュ関数の特徴により初期値と利用関数と現適用回数がわからなければ認識情報の作成が非常に困難であり、上記第１の実施の形態のようにカウンタ利用の場合に比べ透かしキーの偽造は困難となり、セキュリティが高くなる効果が得られる。また、生成されるハッシュ値は、ハッシュ値サイズは固定であるという特徴があるため、透かしキーのサイズに制限があるような電子透かしを使用した場合には制限内に収めるのに有用である。

【００４０】

第３の実施の形態

以下、上記第１の実施の形態との相違点を説明する。本第３の実施の形態は、上記第１の実施の形態と比較して透かしキーに含まれる認証情報の内の画像識別値を画像カウンタのカウント数ではなく、画像ファイルを作成したファイル作成時間とした。

【００４１】

図７に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部２２(m) は、認証情報生成手段２４(m) と透かしキー生成手段２５(m) とを有している。前記認証情報生成手段２４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置を識別するための装置識別値Ｄ24a(m)と、元画像Ａ(m) を識別するための画像識別値Ｄ24

d(m)とを使用する。この画像識別値Ｄ24d(m)が、本第３の実施の形態では、ファイル作成時間としたのである。

【００４２】

このため、前記認証情報生成手段２４(m) には、装置識別値Ｄ24a(m)を記憶する装置識別値記憶部２４ａ(m) と、元画像Ａ(m) をナンバリングするための画像識別値Ｄ24d(m)を元画像Ａ(m) の処理毎のファイル作成時間を刻むタイマ２４ｄ(m) とを備えてある。なお、ファイル作成時間はほぼすべてのファイルシステムにおいて画像ファイルと共に保持されるため、通常は、前記タイマ２４ｄは特別に設ける必要がない。前記透かしキー生成手段２５(m) は、装置識別値Ｄ24a(m)及びファイル作成時間としての画像識別値Ｄ24d(m)を含む透かしキーＢ22(m) を生成する。

【００４３】

図８に、画像管理サーバの認証情報生成手段の機能ブロック構成図を示す。この認証情報生成手段３４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置を識別するための装置識別値Ｄ34a(m)と、元画像Ａ(m) を識別するための画像識別値Ｄ34d(m)とを使用する。この画像識別値Ｄ34d(m)が、本第３の実施の形態では、ファイル作成時間としたのである。

【００４４】

このため、前記認証情報生成手段３４(m) には、装置識別値Ｄ34a(m)を記憶する装置識別値記憶部３４ａ(m) と、元画像Ａ(m) をナンバリングするための画像識別値Ｄ34d(m)を元画像Ａ(m) の処理毎のファイル作成時間を記憶するタイムスタンプ記憶部３４ｄ(m) とを備えてある。なお、ファイル作成時間はほぼすべてのファイルシステムにおいて、ファイル作成時間が画像ファイルに付随する付随情報として画像ファイルとともに転送される。このため、タイムスタンプ記憶部３４ｄ(m) は、通常は設ける必要がない。

【００４５】

なお、上述した前記認証情報生成手段３４(m) は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省略する。

本第３の実施の形態では、画像識別値としてファイル作成時間を使用し、このファイル作成時間により生成した認証情報を含む透かしキーとしたため、上記第１の実施の形態に比べ、画像カウンタが不用になる。なお、通常のファイルシステムのように、ファイル作成時間を誰にでも確認可能な状態で転送すると、セキュリティが低くなるため、暗号化して転送するのが好ましい。

【００４６】

第４の実施の形態

以下、上記第１の実施の形態との相違点を説明する。本第４の実施の形態は、上記第１の実施の形態と比較して透かしキーに含まれる認証情報に元画像の作成者を識別する作成者情報を追加したものである。また、画像処理システムのネットワークは、上記第１の実施の形態の場合を想定し、その説明は省略する。

【００４７】

図９に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部２２(m) は、認証情報生成手段２４(m) と透かしキー生成手段２５(m) とを有している。前記認証情報生成手段２４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。また、透かしキー生成部２５(m) には、元画像Ａ(m) の作成者を認証する作成者認証装置２４ｅ(m) が接続している。この作成者認証装置２４ｅ(m) は、画像処理装置の外部の設けても、内部に設けてもよい。本実施の形態の認証情報には、提供先を識別するための認証情報には、前記提供先識別情報と前記画像識別情報と前記作成者情報がある。ここでは、提供先である画像処理装置を識別するための装置識別値Ｄ24a(m)と、元画像Ａ(m) を識別するための画像識別値Ｄ24b(m)と、元画像の作成者を識別する作成者情報Ｄ24e(m)を使用する。この作成者情報Ｄ24e(m) が、本第３の実施の形態で追加したものである。この作成者情報としては、例えば、作成者ＩＤ、作成者氏名、指紋情報、アイリス情報、顔画像データ等がある。このため、前記画像認証装置２４ｅ(m) は、パスワード認証、指紋認証、アイ

リス認証、顔写真認証等を行う機能を有する必要がある。なお、作成者情報Ｄ24e(m)は、システム運用開始時又は運用中に予め設定しておけばよい。

【００４８】

また、前記認証情報生成手段２４(m) には装置識別値記憶部２４ａ(m) と画像カウンタ２４ｂ(m) とを備えてあり、前記透かしキー生成手段２５(m) は、装置識別値Ｄ24a(m)、画像識別値Ｄ24b(m)及び作成者情報Ｄ24e(m)を含む透かしキーＢ22(m) を生成する。

なお、上述した前記透かしキー生成部２２(m) の認識情報生成手段２４(m) に接続する作成者認証装置２４ｅ(m) は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、画像管理サーバや画像入力装置の説明は省略する。また、画像管理サーバや画像入力装置にも、作成者情報Ｄ24e(m)の設定をシステム運用開始時に予め設定しておけばよい。

【００４９】

本第４の実施の形態によれば、画像取り込み時の偽造防止や改竄発覚時の作成者特定のために画像処理装置において画像処理を行う際に、作成者認証を行い、透かしキー作成情報として作成者情報を含めたため、その原本画像の作成者の特定を行いやすくする。したがって、偽造判明後の作成者の追跡を行いやすくなり、また、画像処理装置を利用して不正な原本画像が作成された場合、作成者の特定を行う追跡調査を容易にし、偽造防止・偽造抑止の効果を大幅に向上させることができる。

【００５０】

つまり、一般的には、画像処理装置の操作時に認証を行い、改竄発覚時にはその認証ログおよび画像処理ログを解析することによって、作成者の特定が行えるシステムでは、ログの改竄等によって作成者特定作業を妨げることが可能であるが、さらに、本実施の形態では、透かしキーに作成者情報を含めたことにより、電子透かしと透かしキーの検証の結果、改竄が検出された場合、改竄者の特定を行うことができるようになる。改竄者といえども改竄者自身の作成者情報を用いない限り、電子透かしを埋め込むことができないからである。

【００５１】

また、複数の許可者がいる場合は、透かしキーの生成を許可者数分行い、検証できた透かしキーを使用するのが一番容易である。このため、作成許可者ＩＤ等と許可者情報のテーブルを画像管理サーバと画像表示装置に登録しておき、作成者情報そのものでなく、作成許可者ＩＤ等の情報を通信によって受け渡し、作成許可者ＩＤから作成許可者情報を検索し、それを透かしキー作成に使用するようにしてもよい。この場合、作成者情報そのものを暗号化して通信によって受け渡すのが好ましい。

【００５２】

さらに、システムが大きい場合は、作成許可者の管理を容易にするために画像処理の作成許可者を登録しておくデータベースである作成許可者データベース装置をシステム内に準備しておくの好ましい。これにより、作成許可者の管理が集中して行え、また、管理場所が一つであるため作成者情報のセキュリティ保持が容易に行える。

【００５３】

なお、作成者情報としては、作成者認証装置やセキュリティ上の考慮からさまざまなタイプのあり、その中でも、例えば、顔写真画像のように大きなサイズのデータの場合に、透かしキーとして使用できるデータサイズに制限があるときには、一方向ハッシュ関数を使用して、大きなデータを固定サイズのハッシュ値に変換し、そのハッシュ値を作成者情報に追加した認証情報を含む透かしキーを使用するのが好ましい。

【００５４】

第５の実施の形態

以下、上記第１の実施の形態との相違点を説明する。本第５の実施の形態は、上記第１の実施の形態と比較して透かしキーに含まれる認証情報の内の装置を特定する装置識別値ではなく、ＬＡＮが敷設してある場合のＭＡＣアドレスを装置識別に使用するようにした。また、画像処理システムのネットワークは、上記第１の実施の形態の場合を想定し、その説明は省略するが、ここでは、特に、画像処理装置と画像管理サーバがＬＡＮで接続されており、ＬＡＮボードが組み込ま

れている場合を想定する。

【００５５】

図１０に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部２２(m) は、認証情報生成手段２４(m) と透かしキー生成手段２５(m) とを有している。前記認証情報生成手段２４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報の内で元画像Ａ(m) を識別するための画像識別値Ｄ24b(m)を生成する機能を有する。また、透かしキー生成部２５(m) には、提供先である画像処理装置を識別するための装置識別値としての自らのＭＡＣアドレスＤ24f(m)を検出するＭＡＣアドレス検出部２４ｆ(m) が接続している。このＭＡＣアドレス検出部２４ｆ(m) は、画像処理装置の外部の設けても、内部に設けてもよい。ＭＡＣアドレスＤ24f(m)は、画像処理装置に固有の番号である。また、前記認証情報生成手段２４(m) には、装置識別値Ｄ24a(m)を記憶する装置識別値記憶部２４ａを備えてある。前記透かしキー生成手段２５(m) は、装置識別値としてのＭＡＣアドレスＤ24f(m)及び画像識別値Ｄ24b(m)を含む透かしキーＢ22(m) を生成する。

【００５６】

なお、本実施の形態では、画像管理サーバや画像表示装置には、予め画像処理装置のＭＡＣアドレスを記憶する記憶部を設ければ、上記第１の実施の形態と同様に、透かしキーが正当なものか否かを判断することができるため、画像管理サーバ及び画像表示装置の説明は省略する。

なお、ＭＡＣアドレスを使用した場合には、透かしキーを送ってきた画像処理装置のＭＡＣアドレスは画像管理サーバで認識可能なため、ＭＡＣアドレスの記憶部を設けなくとも、そのＭＡＣアドレスと透かしキーから分離した装置識別値の比較を行うことが可能である。この場合は、下記第７の実施の形態で説明する。

【００５７】

本第５の実施の形態では、装置識別値としてＭＡＣアドレスを使用した認証情報を含む透かしキーとしたため、装置識別値を新たに設定する必要がない。

第６の実施の形態

以下、上記第１の実施の形態との相違点を説明する。本第６の実施の形態は、上記第１の実施の形態と比較して透かしキーに含まれる認証情報に画像処理装置が所属するシステムを識別するシステム情報を追加したものである。また、画像処理システムのネットワークは、上記第１の実施の形態の場合を想定し、その説明は省略する。

【００５８】

図１１に、画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部２２(m) は、認証情報生成手段２４(m) と透かしキー生成手段２５(m) とを有している。前記認証情報生成手段２４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。また、透かしキー生成部２５(m) には、画像処理装置が所属するシステムを識別するシステム情報D24g(m)を記憶したシステム情報記憶部２４ｇ(m) が接続している。このシステム情報記憶部２４ｇ(m) は、画像処理装置の外部に設けても、内部に設けてもよい。本実施の形態の認証情報には、前記提供先識別情報と前記画像識別情報と前記システム情報がある。ここでは、提供先である画像処理装置を識別するための装置識別値Ｄ24a(m)と、元画像Ａ(m) を識別するための画像識別値Ｄ24b(m)と、システム情報Ｄ24g(m)を使用する。このシステム情報Ｄ24g(m)が、本第６の実施の形態で追加したものであり、システム運用開始時又は運用中に予め設定しておけばよい。なお、画像処理装置が多数の場合には、手間や管理が負担となるため、ソフトウェアのコンパイル時に指定して、ソフトウェア中に取り出し難いように埋め込む方が簡単で安全である。

【００５９】

また、前記認証情報生成手段２４(m) には、装置識別値記憶部２４ａ(m) と画像カウンタ２４ｂ(m) とを備えてある。前記透かしキー生成手段２５(m) は、装置識別値Ｄ24a(m)、画像識別値Ｄ24b(m)及びシステム情報Ｄ24g(m)を含む透かしキーＢ22(m) を生成する。

なお、上述した前記透かしキー生成部２２(m) の認識情報生成手段２４(m) に接続するシステム情報記憶部２４ｇ(m) は、画像管理サーバや画像入力装置にも設ければ、互いに透かしキーが正当なものか否かを判断することができるため、

画像管理サーバや画像入力装置の説明は省略する。

【００６０】

本第６の実施の形態によれば、画像ファイルに電子透かしを埋め込む透かしキーにシステムを識別するシステム情報を含めたため、システム外からの不正行為防止が可能となる。たとえば、本実施の形態によると、同じシステム内での不正に対しての確認や対策だけでなく、同じ方式によって作成された他のシステムの装置やツールを利用しての偽造を判明させるのが容易になる。つまり、同じシステム方式の他のシステムの画像処理装置やソフトウェア処理としてインプリメントされている場合に、たとえば、画像処理ソフトウェアが盗まれたりして不正が行われたときでも、システム毎にシステム情報が異なる為に偽造された原本画像と透かしキーを検証時に発見することができるため、不正利用を防ぐことができるようになる。

【００６１】

第７の実施の形態

図１２は、第７の実施の形態の画像処理システムのネットワーク構成図である。この画像処理システムでは、画像入力装置１０１(1) ～(M) で取り込まれた画像は、画像処理装置１０６(1) ～(M) 、画像管理サーバ１０７及びネットワーク１０４を介して画像表示装置１０８(1) ～(N) のそれぞれで表示されるようになっている。なお、以下の説明では、画像入力装置１０１(1) ～(M) のｍ番目を画像入力装置１０１(m) とし、画像処理装置１０６(1) ～(M) のｍ番目を画像処理装置１０６(m) とし、画像表示装置１０８(1) ～(N) のｎ番目を画像表示装置１０８(n) とする。ここでは、特に、画像処理装置１０６(m) と画像管理サーバ１０７が図示しないＬＡＮで接続されており、ＬＡＮボードが組み込まれている場合を想定する。

【００６２】

前記画像入力装置１０１(m) は、画像を取り込んで電子データ化する装置であり、通常スキャナや電子カメラによって構成され、取り込まれた画像データを元画像Ａ(m) として出力する。

前記画像処理装置１０６(m) は、前記画像入力装置１０１(m) からの元画像Ａ

(m) をそれぞれ入力し、この元画像Ａ(m) に電子透かしを埋め込んだ原本画像Ｃ(m) を出力する機能を有する。

【００６３】

図１３に、第７の実施の形態の画像処理装置の機能ブロック構成図を示す。この画像処理装置１０６(m) は、電子透かし埋め込み部６１(m) と透かしキー生成部６２(m) とＭＡＣアドレス検出部６４ｄ(m) とを有している。前記電子透かし埋め込み部６１(m) は、元画像Ａ(m) に対する改竄を検出するための電子透かしを透かしキーＢ62(m) を用いて元画像Ａ(m) に埋め込んだ原本画像Ｃ(m) を出力する。前記透かしキー生成部６２(m) は、前記透かしキーＢ22(m) を生成する。ここで、透かしキーＢ62(m) は、本実施の形態では、電子透かしの埋め込み・検証の両方に使用できる共通キーとして説明するが、埋め込みと検証とが相違するようにしてもよい。

【００６４】

なお、上記第１の実施の形態の説明と同様に、本第７の実施の形態でも透かしキーＢ62(m) の生成にＲＳＡ等の公開鍵システムを用いて、透かしキーＢ62(m) のやり取りを行う場合を想定する。

図１４に、第７の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図を示す。この透かしキー生成部６２(m) は、認証情報生成手段６４(m) と透かしキー生成手段６５(m) とを有している。前記認証情報生成手段６４(m) は、正当な提供先からの画像ファイルであることを認証する認証情報を生成する機能を有する。認証情報は、画像ファイルの提供先を識別するための提供先識別情報と画像ファイルを識別する画像識別情報とがある。ここでは、提供先である画像処理装置１０６(m) を識別するためのＭＡＣアドレスD64d(m)と元画像Ａ(m) を識別するための画像識別値D64b(m)とを使用する。また、認証情報生成手段６４(m) には、元画像Ａ(m) をナンバリングするための画像識別値D64b(m)を元画像Ａ(m) の処理毎に繰り上がるカウント数として出力する画像カウンタ６４ｂ(m) とを備えてある。前記透かしキー生成手段６５(m) は、ＭＡＣアドレスD64d(m)と画像識別値D64b(m)とを含む透かしキーＢ62(m) を生成する。例えば、ＭＡＣアドレスD64d(m)を「00:AB:20:CD:40:EF 」とし、画像識別値D64b(m)を「

0x00000001」とした場合、それぞれを組み合わせた「0x00AB20CD40EF00000001」を含む透かしキーＢ62(m) を生成する。なお、上記第４の実施の形態で説明した作成者情報Ｄ24e(m)を含めた透かしキーＢ62(m) の場合には、例えば、ＭＡＣアドレスＤ64d(m)を「00:AB:20:CD:40:EF 」とし、画像識別値Ｄ64b(m)を「0x01234567」とし、作成者情報Ｄ24e(m)の１６進データを「0x89AB01BE9859」とした場合、それぞれを組み合わせた「0x00AB20CD40EF0123456789AB01BE9859」を含む透かしキーＢ62(m) を生成する。作成者情報Ｄ24e(m)の１６進データが長い場合には、例えば、「0xFF0122CFAA234C5688FE0100EF0100EFA289EF」のハッシュ値にして、「0x00AB20CD40EF0123456789AB01BE9859FF0122CFAA234C5688FE0100EF0100EFA289EF」を含む透かしキーＢ62(m) を生成する。

【００６５】

図１３に戻って、前記ＭＡＣアドレス検出部６４ｄ(m) は、画像処理装置１０６(m) 自体のＭＡＣアドレスＤ64d(m)を検出する。そして、画像処理装置１０６(m) は、原本画像Ｃ(m) を出力する。

図１２に戻って、前記画像管理サーバ１０７は、前記画像処理装置１０６(m) から送られてきた原本画像Ｃ(m) を保存・管理するサーバであり、通常のデータベースやワークフローシステムとして構築される。

【００６６】

図１５に、第７の実施の形態の画像管理サーバの機能ブロック構成図を示す。この画像管理サーバ１０７は、ＭＡＣアドレス検出部７０と、電子透かし検証部７１と、透かしキー生成部７２と、この透かしキー生成部７２内に備える認証情報生成手段７４(1) ～(M) （以下、ｍ番目を認証情報生成手段７４(m) という。）及び透かしキー生成手段７５と、記憶制御部７７と、ファイル名作成部９０と、ＭＡＣアドレスデータベース９１とを有している。前記ＭＡＣアドレス検出部７０は、提供先である画像処理装置１０６(m) を識別するための前記画像処理装置１０６(m) のＭＡＣアドレスＤ64d(m)を検出する。前記電子透かし検証部７１は、画像処理装置１０６(m) から提供された原本画像Ｃ(m) を生成された透かしキーＢ72(m) を用いて電子透かしが抽出できるか否かを検証する。原本画像Ｃ(m) から電子透かしを抽出できなければ原本画像Ｃ(m) に改竄が行われているとい

うことが分かり、抽出できれば改竄が行われていないということが分かる。前記透かしキー生成部７２は、透かしキーＢ72(m) を生成する機能を有し、前記認証情報生成手段７４(m) と透かしキー生成手段７５とを備えている。前記認証情報生成手段７４(m) は、元画像Ａ(m) をナンバリングするための画像識別値Ｄ74b(1)～(M) （以下、m番目を画像識別値Ｄ74b(m)という。）を原本画像Ｃ(m) の処理毎に繰り上がるカウント数として出力する画像カウンタ７４ｂ(m) とを備えてある。なお、画像カウンタ７４ｂ(m) のセットは、システム運用開始時又は運用中に予め行っておく。前記透かしキー生成手段７５は、前記ＭＡＣアドレス検出部７０が検出したＭＡＣアドレスＤ64d(m)と画像識別値Ｄ74b(m)とを含む透かしキーＢ72(m) を生成する。

【００６７】

前記記憶制御部７７は、原本画像Ｃ(m) とこれに付随する情報としてのファイル名Ｆ(m) を管理する。前記ファイル名作成部９０は、画像処理装置１０６(m) のＭＡＣアドレスＤ64d(m)に基づくファイル名Ｆ(m) を作成する。前記ＭＡＣアドレスデータベース９１は、ＭＡＣアドレスＤ64d(m)に基づくファイル名Ｆ(m) の定義テーブルを格納してある。したがって、ファイル名作成部９０は、ＭＡＣアドレスＤ64d(m)に基づくファイル名Ｆ(m) をＭＡＣアドレスデータベース９１から得ることができる。なお、ファイル名作成部９０が一定の定義式に基づきその都度ファイル名Ｆ(m) を作成するようにしてもよい。そして、画像管理サーバ１０７は、原本画像Ｃ(m) とともにファイル名Ｆ(m) を付随させて、各画像表示装置１０８(n) に送る（図１２参照）。

【００６８】

図１２に戻って、前記ネットワーク１０４は、例えば、ＬＡＮやＷＡＮ等で構築されるネットワークである。前記画像表示装置１０８(n) は、原本画像Ｃ(m) を表示利用する装置である。

図１６に、第７の実施の形態の画像表示装置の機能ブロック構成図を示す。この画像表示装置１０８(n) は、電子透かし検証部８１(n) と、透かしキー生成部８２(n) と、この透かしキー生成部８２(n) 内に備える認証情報生成手段８４(1)～(M) （以下、m番目を認証情報生成手段７４(m) という。）及び透かしキー

生成手段８５(n) と、表示制御部８９(n) と、ＭＡＣアドレスデータベース９１(n) と、ファイル名処理部９２(n) とを有している。前記電子透かし検証部８１(n) は、画像管理サーバ１０７から提供された原本画像Ｃ(m) を生成した透かしキーＢ72(m) を用いて電子透かしが抽出できるか否かを検証する。原本画像Ｃ(m) から電子透かしを抽出できなければ原本画像Ｃ(m) に改竄が行われているということが分かり、抽出できれば改竄が行われていないということが分かる。前記透かしキー生成部８２(n) は、透かしキーＢ72(m) を生成する機能を有し、前記認証情報生成手段８４(m) と透かしキー生成手段８５(n) とを備えている。前記認証情報生成手段８４(m) は、元画像Ａ(m) をナンバリングするための画像識別値Ｄ74b(1)～(M) （以下、ｍ番目を画像識別値Ｄ74b(m)という。）を原本画像Ｃ(m) の処理毎に繰り上がるカウント数として出力する画像カウンタ８４ｂ(m) とを備えてある。なお、画像カウンタ８４ｂ(m) のセットは、システム運用開始時又は運用中に予め行っておく。前記透かしキー生成手段８５は、前記ファイル名処理部９２(n) からのＭＡＣアドレスＤ64d(m)と画像識別値Ｄ84b(m)とを含む透かしキーＢ72(m) を生成する。なお、画像識別値Ｄ84b(m)は、前記画像識別値Ｄ74b(m)と同一になるように設定してある。前記ＭＡＣアドレスデータベース９１(n) は、ＭＡＣアドレスＤ64d(m)に基づくファイル名Ｆ(m) の定義テーブルを格納してある。前記ファイル名処理部９２(n) は、ＭＡＣアドレスデータベース９１(n) を参照して、ファイル名Ｆ(m) から画像処理装置１０６(m) のＭＡＣアドレスＤ64d(m)を得る。なお、ファイル名作成部９２(n) が一定の定義式に基づきその都度ファイル名Ｆ(m) からＭＡＣアドレスデータベース９１(n) を参照して、画像処理装置１０６(m) のＭＡＣアドレスＤ64d(m)を得るようにしてもよい。前記表示制御部５９(n) は、提供された原本画像Ｃ(m) を図示しないＣＲＴ等の表示部に表示させる。

【００６９】

次に、上記構成の画像処理システムの画像処理の流れを説明する。図１２～図６を適宜参照するものとする。

まず、画像入力装置１０１(m) によって取り込まれた電子データ化した元画像Ａ(m) は、画像処理装置１０６(m) に入力される。

次に、画像処理装置１０６(m) では、透かしキー生成部６２(m) で電子透かしの埋め込みのための透かしキーB62(m) を生成し、その透かしキーB62(m) を使用して電子透かし埋め込み部６１(m) で電子透かしを埋め込んだ原本画像C(m) を生成する。また、画像処理装置１０６(m) では、MACアドレス検出部６４d(m) が、自らのMACアドレスD64d(m)を検出して、そのMACアドレスD64d(m)の一部又は全部を透かしキーB62(m) に含めるようになっている。そして、画像処理装置１０６(m) は、原本画像C(m) を画像管理サーバ１０７に送る。

【００７０】

次に、画像管理サーバ１０７では、MACアドレス検出部７０が画像処理装置１０６(m) のMACアドレスD64d(m)を検出し、透かしキー生成手段７５がそのMACアドレスD64d(m)を含む透かしキーB72(m) を生成し、電子透かし検証部７１がその生成した透かしキーB72(m) を使用して原本画像C(m) の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像C(m) の改竄が行われていないということの確認を行う。そして、前記画像表示装置１０８(n) から原本画像C(m) の転送を要求されたり自動的に転送する場合には、画像管理サーバ１０７は、画像処理装置１０６(m) のMACアドレスD64d(m)に基づいたファイル名F(m) を原本画像C(m) に付随させて各画像表示装置１０８(n) に送る。

【００７１】

各画像表示装置１０８(n) では、送られてきたファイル名F(m) から画像処理装置１０６(m) のMACアドレスD64d(m)を得て、透かしキー生成手段８５(n) がこのMACアドレスD64d(m)を含む透かしキーB72(m) を生成し、電子透かし検証部８１(n) がその生成した透かしキーB72(m) を使用して原本画像C(m) の電子透かしの検証を行い、抽出できた場合には、送られてきた原本画像C(m) の改竄が行われていないということの確認を行う。そして、前記表示制御部５９(n) は、原本画像C(m) を図示しないCRT等の表示部に表示させる。

【００７２】

したがって、画像表示装置１０８(n) は、電子透かしが抽出できない場合や電子透かしが抽出できたが改竄が検出された場合には、その原本画像C(m) は正当なものでないため、改竄検出の警告を表示等により報知して、その原本画像C(m

）の表示を行わないことで、改竄画像による不正を防止できる。

上記第７の実施の形態によれば、画像管理サーバから画像表示装置へは、認証情報に基づく付随情報を画像ファイルに付随させて受け渡すようにしたため、画像表示装置でも透かしキーを生成することが可能になる。なお、画像処理装置から画像管理サーバの場合も同様に受け渡すようにしてもよい。また、画像処理装置から画像管理サーバの場合では、ＬＡＮ接続されている場合を想定したため、透かしキーの認証情報としてＭＡＣアドレスを使用すると、画像管理サーバはＭＡＣアドレスの受け取りをシステムを変更せずに、ＬＡＮ上で行うことができる。

【００７３】

第８の実施の形態

図１７は、第８の実施の形態の画像処理システムのネットワーク構成図である。この画像処理システムでは、画像入力装置１０１(m) で取り込まれた画像は、画像処理装置１１０(m) 、画像管理サーバ１２０及びネットワーク１０４を介して画像表示装置１３０(n) のそれぞれで表示されるようになっている。なお、以下の説明では、(m) 及び(n) は、上記各実施の形態で使用したのと同一の意味で使用するものとする。

【００７４】

前記画像入力装置１０１(m) は、画像を取り込んで電子データ化する装置であり、通常スキャナや電子カメラによって構成され、取り込まれた画像データを元画像Ａ(m) として出力する。

前記画像処理装置１１０(m) は、前記画像入力装置１０１(m) からの元画像Ａ(m) をそれぞれ入力し、この元画像Ａ(m) に電子透かしを埋め込んだ原本画像Ｈ(m) を出力する機能を有する。このため、電子透かし埋め込み部１１２(m) と透かしキー生成部１１１(m) とを有している。前記電子透かし埋め込み部１１２(m) は、元画像Ａ(m) に対する改竄を検出するための電子透かしを透かしキーＧ111(m)を用いて元画像Ａ(m) に埋め込んだ原本画像Ｈ(m) を出力する。前記透かしキー生成部１１１(m) は、上記各実施の形態で説明した認証情報を含む前記透かしキーＧ111(m)を生成する。ここで、透かしキーＧ111(m)は、本実施の形態では

、電子透かしの埋め込み・検証の両方に使用できる共通キーとして説明するが、埋め込みと検証とが相違するようにしてもよい。なお、上記実施の形態と同様に、透かしキーG111(m)の生成にＲＳＡ等の公開鍵システムを用いて、透かしキーG111(m)のやり取りを行う場合を想定する。

【００７５】

前記画像管理サーバ１２０は、前記画像処理装置１１０(m) から送られてきた原本画像H(m) を保存・管理するサーバであり、通常のデータベースやワークフローシステムとして構築され、電子透かし埋め込み部１２２(m) と透かしキー生成部１２１(m) とを有している。前記電子透かし埋め込み部１２２(m) は、原本画像H(m) に対する改竄を検出するための電子透かしを透かしキーG121(m)を用いて抽出して検証する。前記透かしキー生成部１２１(m) は、前記透かしキーG111(m)と同一の前記透かしキーG121(m)を生成する。なお、透かしキー生成部１２１(m) 内の図示しない装置識別値記憶部への記憶や図示しない画像カウンタのセット等は、システム運用開始時又は運用中に予め行っておく。

【００７６】

前記ネットワーク１０４は、例えば、ＬＡＮやＷＡＮ等で構築されるネットワークである。

前記画像表示装置１３０(n) は、原本画像C(m) を表示利用する装置であり、電子透かし埋め込み部１３２(n) と透かしキー生成部１３１(n) とを有している。前記電子透かし埋め込み部１３２(n) は、原本画像H(m) に対する改竄を検出するための電子透かしを透かしキーG131(m)を用いて抽出して検証する。前記透かしキー生成部１３１(n) は、前記透かしキーG111(m)と同一の前記透かしキーG131(m)を生成する。なお、透かしキー生成部１３１(n) 内の図示しない装置識別値記憶部への記憶や図示しない画像カウンタのセット等は、システム運用開始時又は運用中に予め行っておく。

【００７７】

上述した構成では、画像管理サーバ１１０(m) は、透かしキー生成部１２１(m) によって自ら認証情報を含む透かしキーG111(m)と同一の透かしキーG121(m)を生成し、電子透かし検証部１２２(m) がその透かしキーG121(m)を用いて原本

画像Ｈ(m) から電子透かしを抽出し、改竄の有無を検証して、図示しない記憶制御部に原本画像Ｈ(m) を記憶する。また、同様に、画像表示装置１３０(n) は、透かしキー生成部１３１(n) によって自ら認証情報を含む透かしキーＧ111(m)と同一の透かしキーＧ131(m)を生成し、電子透かし検証部１３２(n) がその透かしキーＧ131(m)を用いて原本画像Ｈ(m) から電子透かしを抽出し、改竄の有無を検証して、図示しない表示部に原本画像Ｈ(m) を表示する。

【００７８】

したがって、上記第８の実施の形態によれば、画像処理装置から画像管理サーバ、又は、画像管理サーバから画像表示装置へ透かしキーを送る必要が無いため、画像処理装置のＭＡＣアドレスや装置シリアル番号などの装置識別値を画像表示装置にシステム運用開始時に登録しておくだけで、画像表示時には画像管理サーバから画像表示装置に原本画像が送られ、画像表示装置で表示することができるようになる。例えば、ワークフローとして画像入力装置から画像管理サーバ、画像表示装置へと一連の流れとして送られ表示される場合と、画像表示装置から画像管理サーバに特定画像要求あって表示される場合のように、互いに原本画像の転送だけ行えば、画像表示装置での表示を行えるため、転送処理の時間の短縮に繋がる。

【００７９】

なお、上記各実施の形態で説明した透かしキー生成部であれば増加するソフトウェアまたはハードウェアも僅かなもので構成することができる。また、透かしキーを搾取可能な場所が減少することにより、システムとしてセキュリティレベルが向上するという効果が挙げられる。

また、上記各実施の形態では、画像管理サーバが一台の場合を想定して説明したが、複数の画像処理装置に対して画像管理サーバも複数ある場合は、システム構成が複雑になるが、画像処理回数を一括管理するサーバをシステム内に置くようにすれば同様に行うことができる。また、それぞれの画像処理装置での画像処理回数が判れば、画像管理サーバが複数であっても上記実施方法が適用できる。画像が送られてきた場合は、画像処理サーバが画像処理回数を問い合わせし、画像処理回数からハッシュ値である画像識別値の生成を行い、その画像識別値から

透かしキーを生成して検証を行い、検証が成功すれば原本画像と透かしキーを対で保存するようにすればよい。

【００８０】

【発明の効果】

以上説明したように本発明の画像処理システムによると、画像ファイルをやりとりする互いの装置でのみ判断できる正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーを用いて、電子透かし情報を埋め込んだ画像ファイルからを電子透かし情報を抽出できるようにしたため、画像ファイルの改竄の有無を判断することができる効果が得られる。

【００８１】

したがって、特権ユーザーによる改竄を防止することができるようになり、画像を扱うすべての装置の完全なアクセス権設定作業を低コストで実現できる効果が得られる。

また、画像ファイル自体を暗号化する必要がなくなるために、従来のように画像の表示毎に復号化（及び再暗号化）の処理を行わなくてもよくなる。このため、特に、多量の画像を処理するシステムではその処理負荷を小さくでき、画像がシステム内に分散した複数のマシンで利用されるシステムでは、画像の管理が万全となってセキュリティの甘いマシンでの不正を防止できるようになる。

【００８２】

さらに、検証データの管理に関しての暗号システムがなくても、画像の改竄を検出できるため、暗号システム自体の管理が高いセキュリティでなくてもよくなる。

したがって、本発明では、画像ファイルの改竄を防止し、画像ファイルの改竄を容易に検出し、画像ファイルの処理負荷を小さくした画像処理システムを低コストで提供することができる。

【図面の簡単な説明】

【図１】

第１の実施の形態の画像処理システムのネットワーク構成図

【図２】

第１の実施の形態の画像処理装置の機能ブロック構成図

【図３】

第１の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図４】

第１の実施の形態の画像管理サーバの機能ブロック構成図

【図５】

第１の実施の形態の画像表示装置の機能ブロック構成図

【図６】

第２の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図７】

第３の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図８】

第３の実施の形態の認証情報生成手段の機能ブロック構成図

【図９】

第４の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図１０】

第５の実施の形態の画像管理サーバの透かしキー生成部の機能ブロック構成図

【図１１】

第６の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図１２】

第７の実施の形態の画像処理システムのネットワーク構成図

【図１３】

第７の実施の形態の画像処理装置の機能ブロック構成図

【図１４】

第７の実施の形態の画像処理装置の透かしキー生成部の機能ブロック構成図

【図１５】

第７の実施の形態の画像管理サーバの機能ブロック構成図

【図１６】

第７の実施の形態の画像表示装置の機能ブロック構成図

【図１７】

第８の実施の形態の画像処理システムのネットワーク構成図

【符号の説明】

１０１　画像入力装置

１０２　画像処理装置

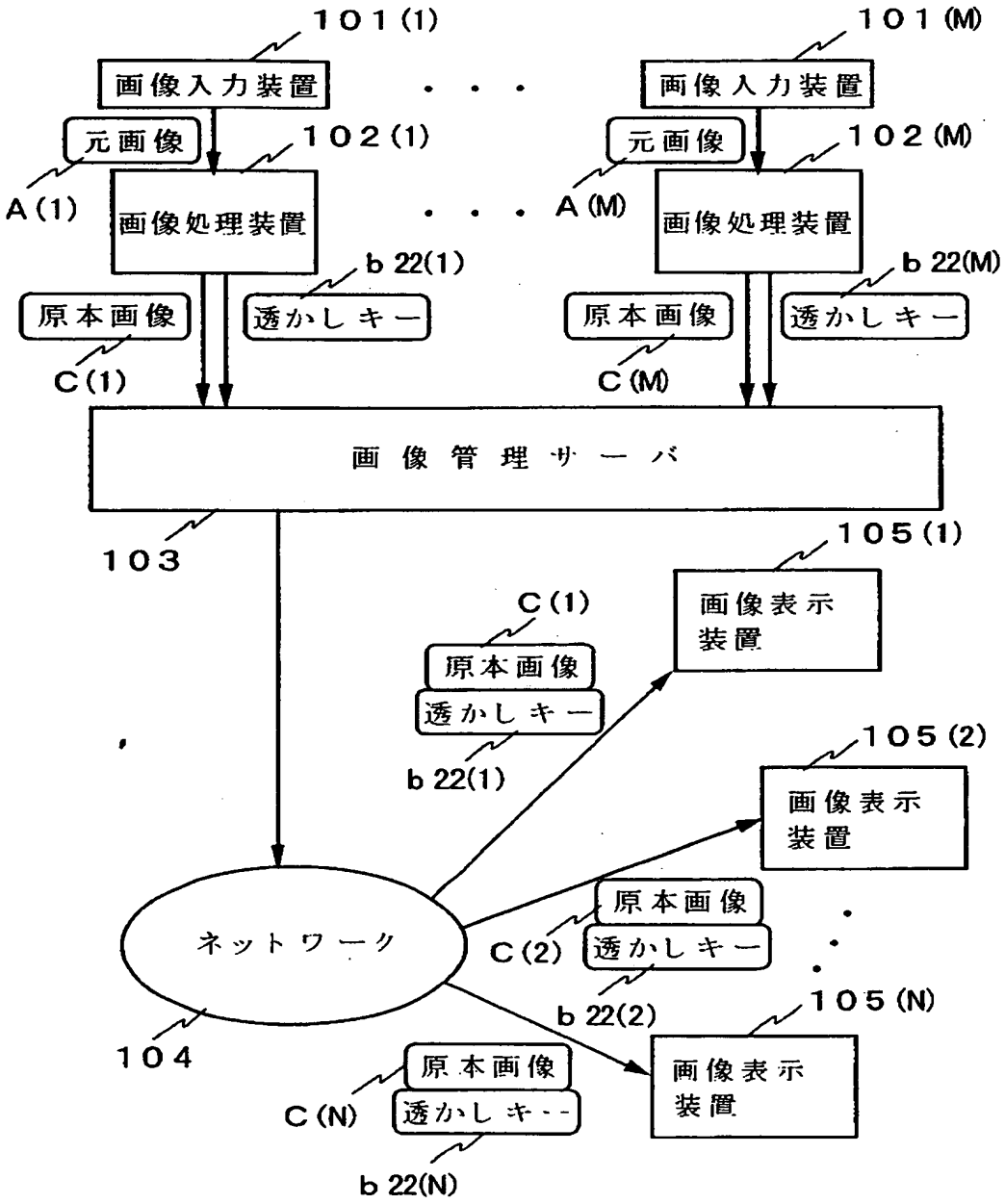
１０３　画像管理サーバ

１０４　ネットワーク

１０５　画像表示装置

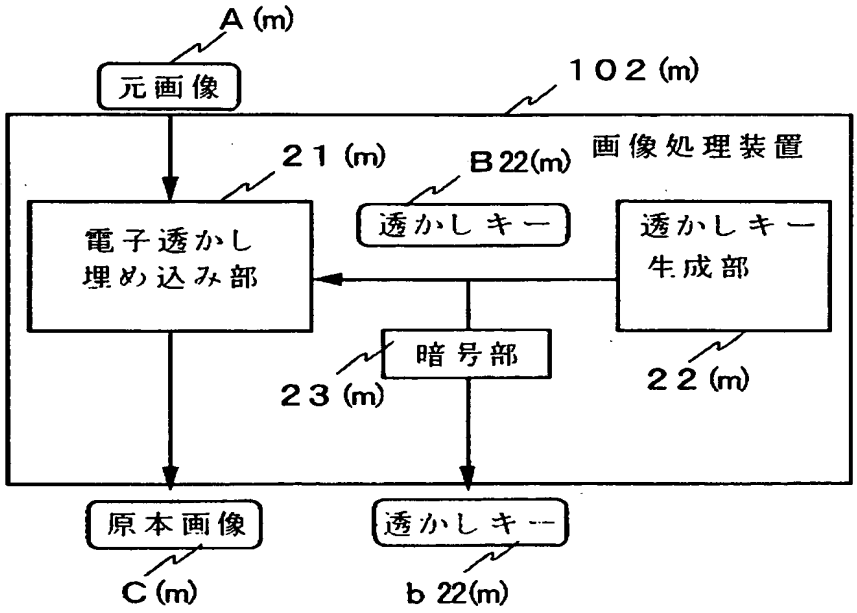
【書類名】　図面

【図１】



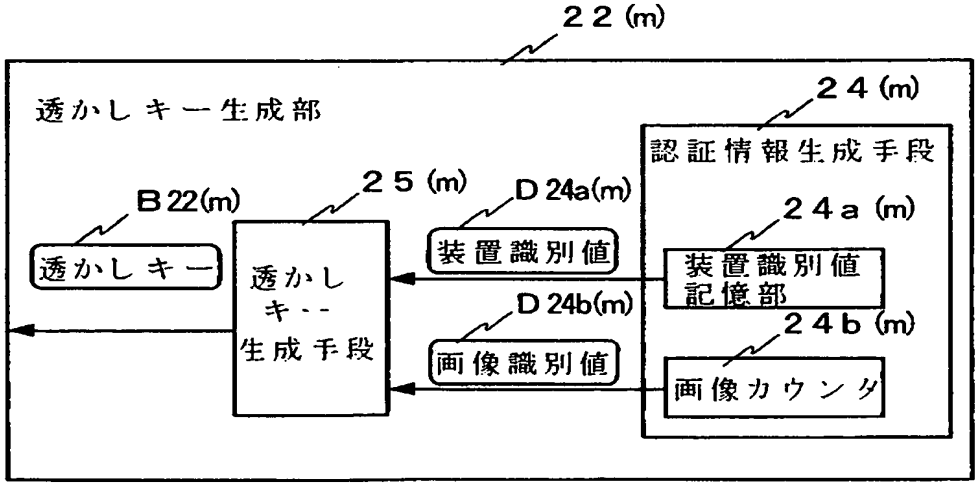
第1 の実施の形態の画像処理システムのネットワーク構成図

【図２】



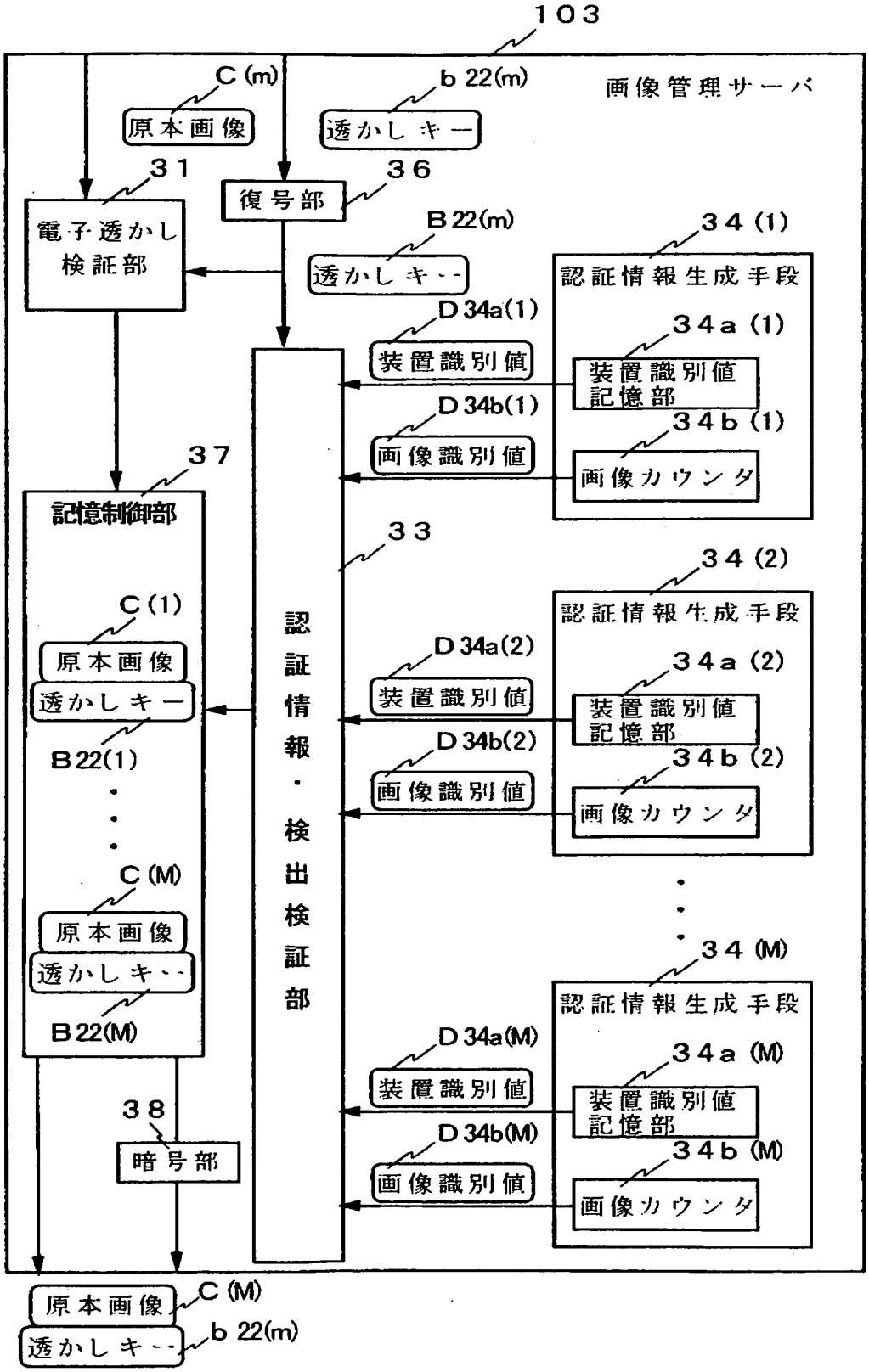
第1 の実施の形態の画像処理装置の機能ブロック構成図

【図３】



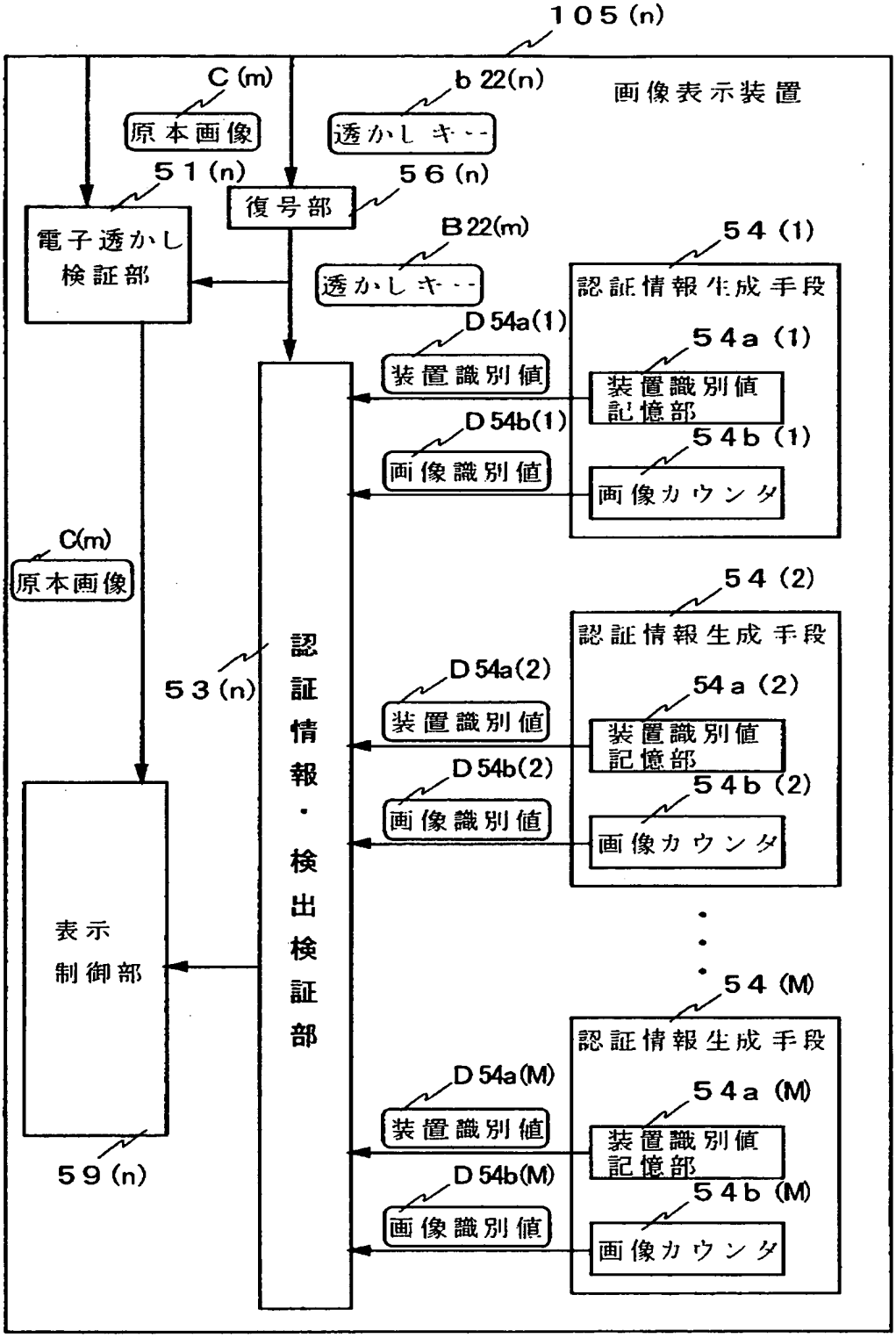
第1 の実施の形態の透かしキー生成部の機能ブロック構成図

【図４】



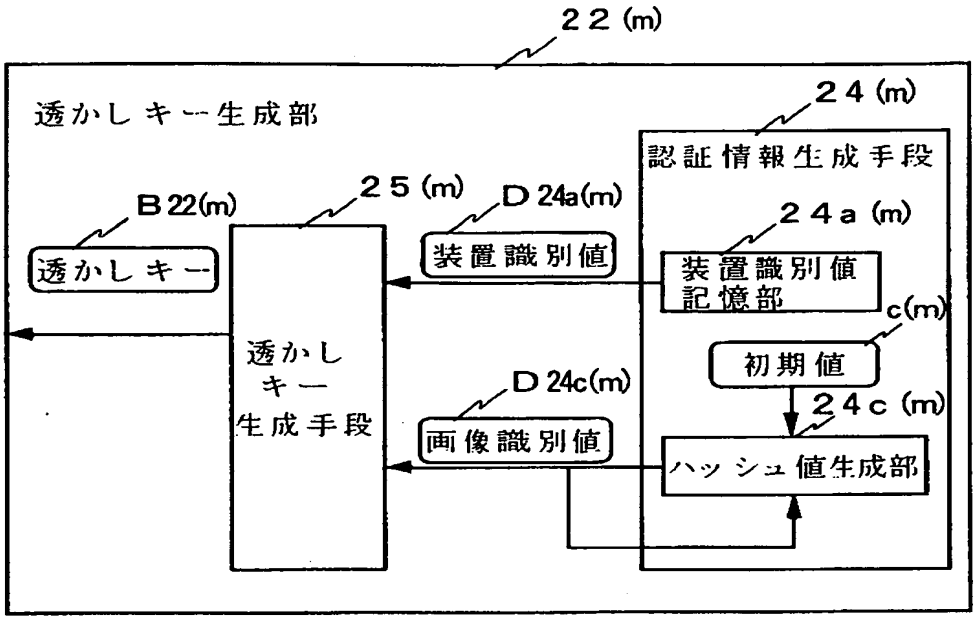
第1の実施の形態の画像管理サーバの機能ブロック構成図

【図５】



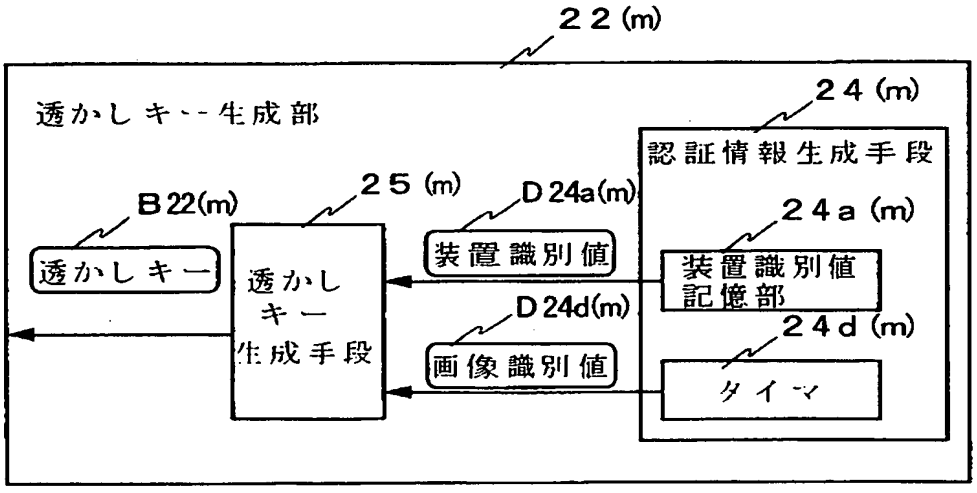
第1 の実施の形態の画像表示装置の機能ブロック構成図

【図６】



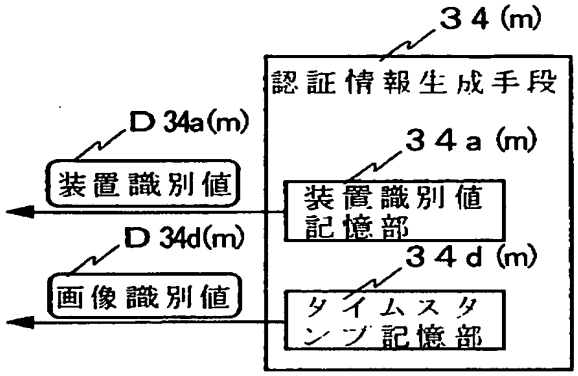
第2 の実施の形態の透かしキー生成部の機能ブロック構成図

【図７】



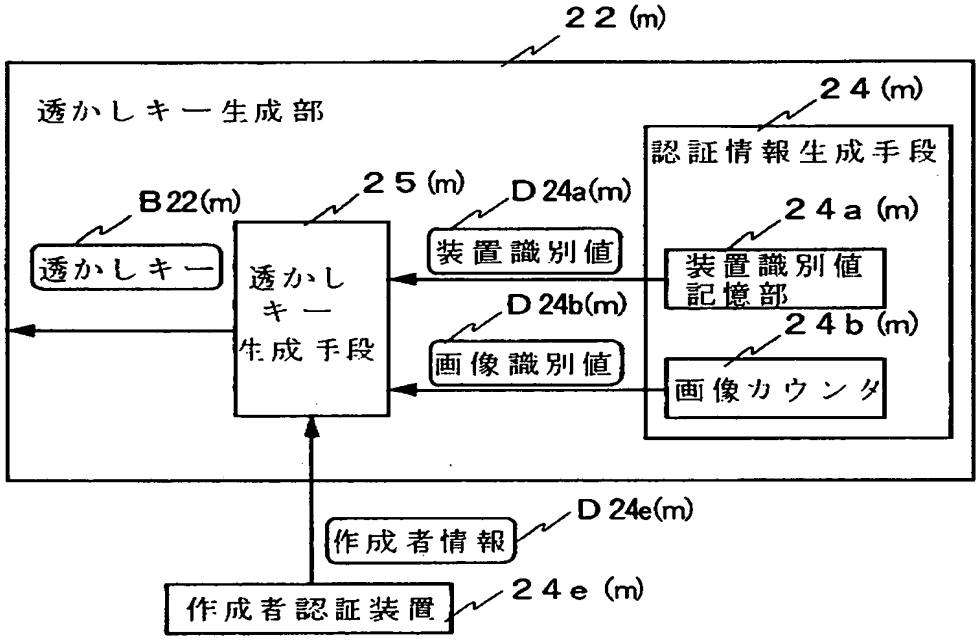
第3 の実施の形態の透かしキー生成部の機能ブロック構成図

【図８】



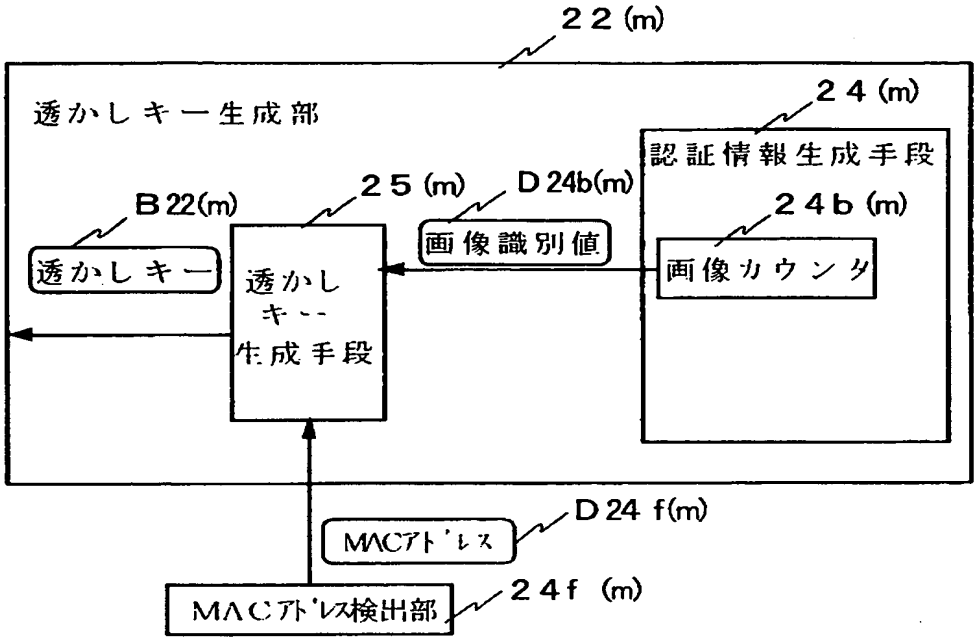
第3の実施の形態の認証情報生成手段の機能ブロック構成図

【図９】



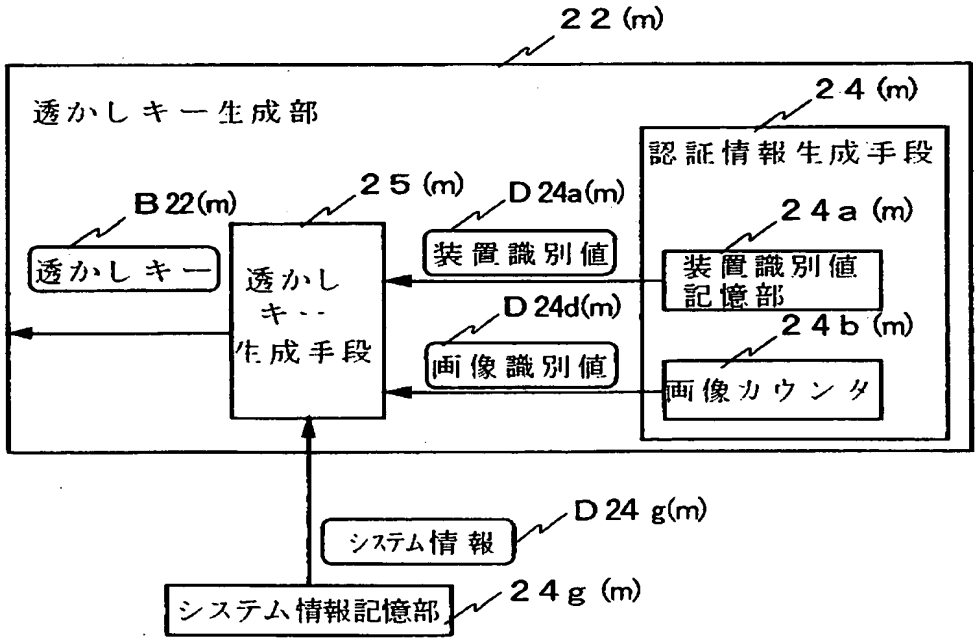
第4の実施の形態の透かしキー生成部の機能ブロック構成図

【図１０】



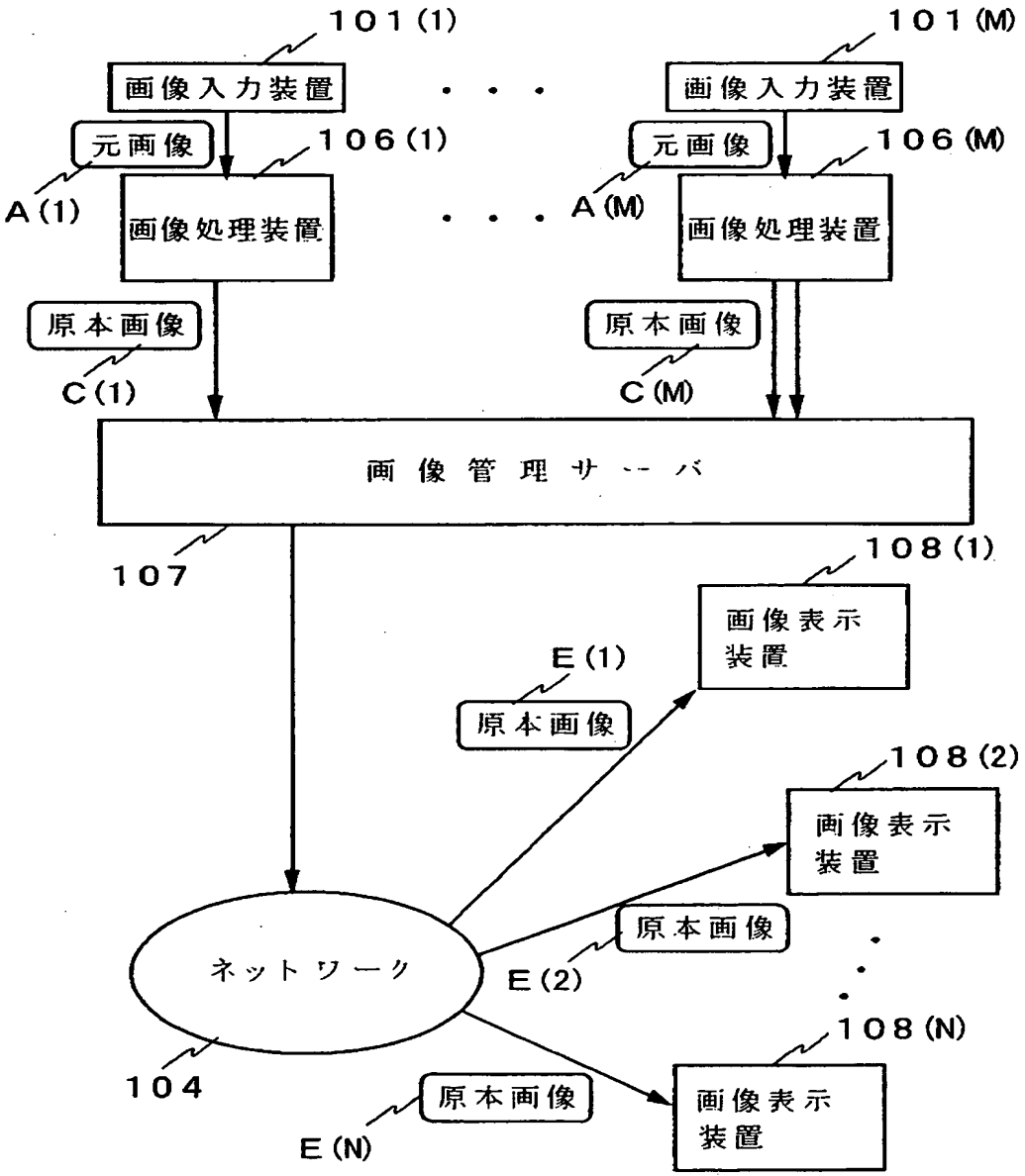
第5の実施の形態の透かしキー生成部の機能ブロック構成図

【図１１】



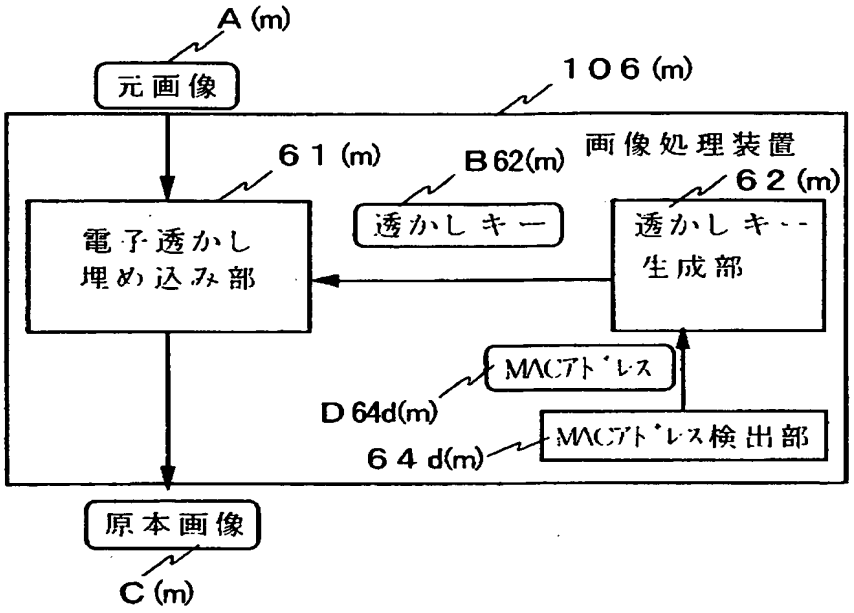
第6の実施の形態の透かしキー生成部の機能ブロック構成図

【図１２】



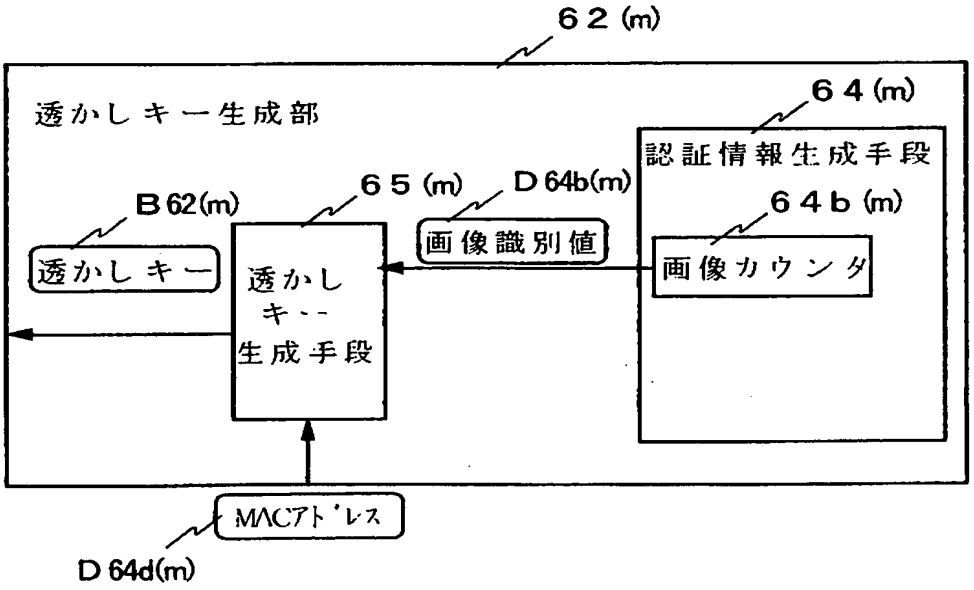
第7 の実施の形態の画像処理システムのネットワーク構成図

【図１３】



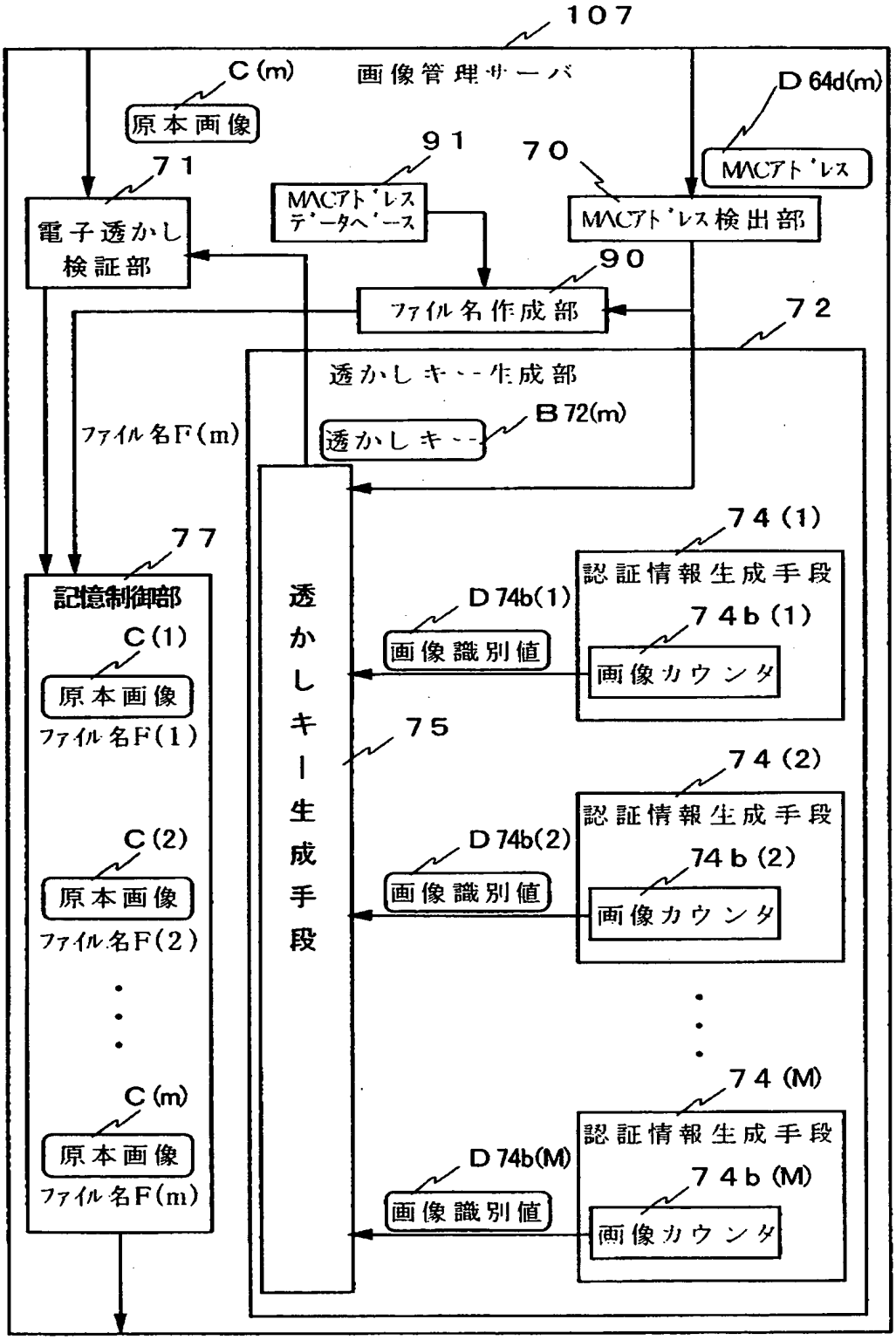
第7 の実施の形態の画像処理装置の機能ブロック構成図

【図１４】



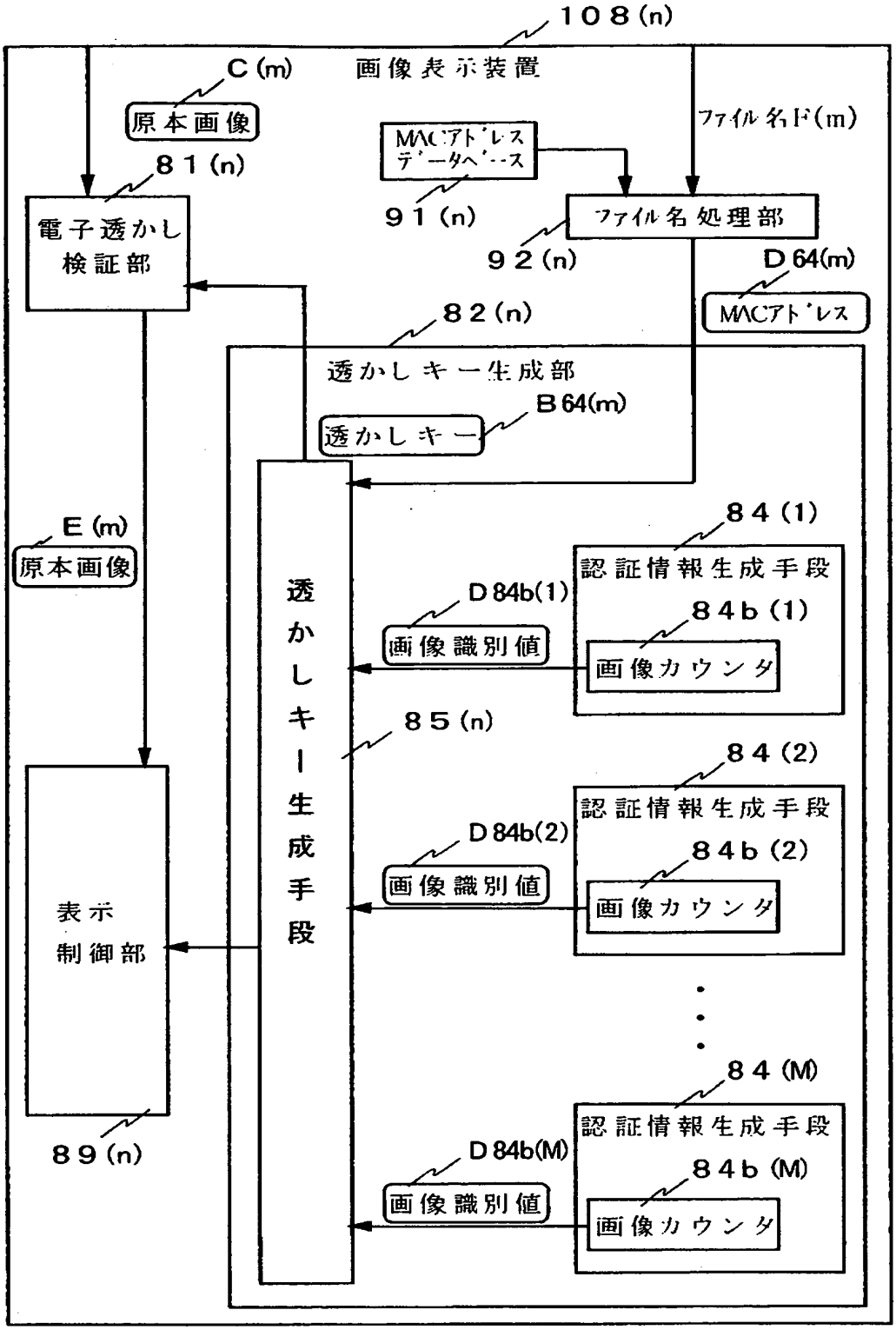
第7 の実施の形態の透かしキー生成部の機能ブロック構成図

【図１５】



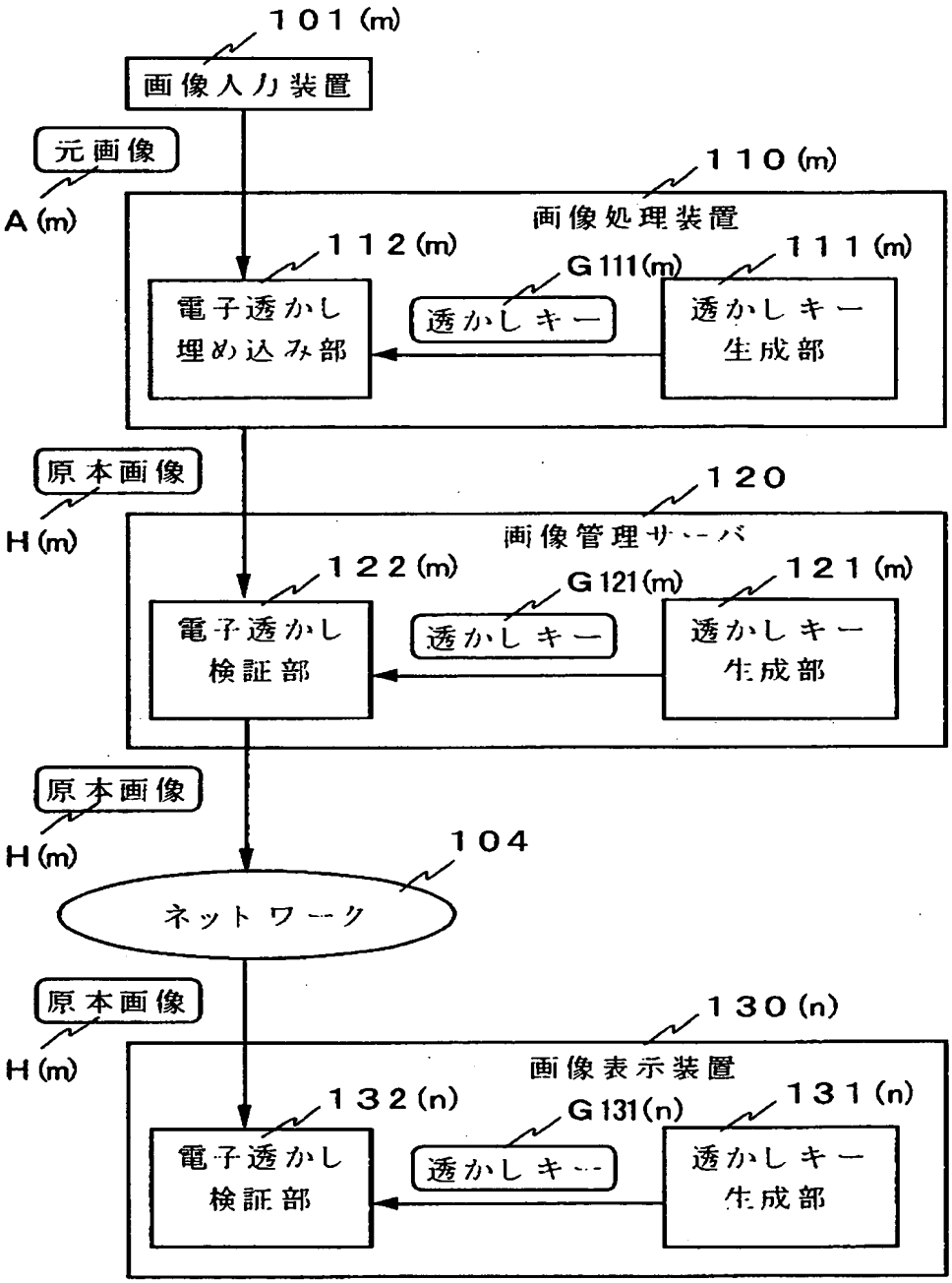
第7の実施の形態の画像管理サーバの機能ブロック構成図

【図１６】



第7 の実施の形態の画像表示装置の機能ブロック構成図

【図１７】



第8の実施の形態の画像処理システムのネットワーク構成図

【書類名】　　要約書

【要約】

【課題】　画像ファイルの改竄を防止し、画像ファイルの改竄を容易に検出し、画像ファイルの処理負荷を小さくした画像処理システムを低コストで提供する。

【解決手段】　正当な提供先からの画像ファイルであることを認証する認証情報を含む透かしキーｂ22(1) を生成し、この透かしキーｂ22(1) を用いて抽出可能な電子透かし情報を元画像Ａ(1) に埋め込んだ原本画像Ｃ(1) と透かしキーｂ22(1) を提供する画像処理装置１０２(1) と、前記画像提供装置１０２(1) から提供された透かしキーｂ22(1) を用いて前記画像提供装置１０２(1) から提供された原本画像Ｃ(1) から電子透かし情報を抽出し、透かしキーｂ22(1) の認証情報を用いて、透かしキーｂ22(1) の改竄の有無を判断した透かしキーｂ22(1) を用いて原本画像Ｃ(1) の改竄の有無を判断し、改竄の有無を判断した原本画像Ｃ(1) と前記透かしキーｂ22(1) を記憶しておき、適宜原本画像Ｃ(1) と透かしキーｂ22(1) を利用先に提供する画像管理サーバ１０３と、この画像管理サーバ１０３から提供された透かしキーｂ22(1) を用いて提供された原本画像Ｃ(1) から電子透かし情報を抽出し、透かしキーｂ22(1) の認証情報を用いて、透かしキーｂ22(1) の改竄の有無を判断した透かしキーｂ22(1) を用いて原本画像Ｃ(1) の改竄の有無を判断し、改竄の有無を判断した原本画像Ｃ(1) を表示利用する画像表示装置とを備えた画像処理システムを提供する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２９５〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　　東京都港区虎ノ門１丁目７番１２号
氏　名　　沖電気工業株式会社